UNIVERSIDADE FEDERAL DO PARANÁ
SETOR DE CIÊNCIAS SOCIAIS APLICADAS
CENTRO DE PESQUISA E PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO
MESTRADO EM ADMINISTRAÇÃO
ÁREA DE CONCENTRAÇÃO: ESTRATÉGIA E ORGANIZAÇÕES

DISSERTAÇÃO DE MESTRADO

RISCO OPERACIONAL E GOVERNANÇA EM PROCESSOS DE TECNOLOGIA DA INFORMAÇÃO DE ORGANIZAÇÕES DE ALTA CONFIABILIDADE: ESTUDO NO BANCO CENTRAL DO BRASIL

PAULO SÉRGIO ROSA

CURITIBA
2008

PAULO SÉRGIO ROSA

RISCO OPERACIONAL E GOVERNANÇA EM PROCESSOS DE TECNOLOGIA DA INFORMAÇÃO DE ORGANIZAÇÕES DE ALTA CONFIABILIDADE: ESTUDO NO BANCO CENTRAL DO BRASIL

Dissertação apresentada como requisito parcial à obtenção do grau de Mestre em Administração – Setor de Ciências Sociais Aplicadas da Universidade Federal do Paraná.

Orientador: Profª Drª Ana Paula Mussi Szabo Cherobim

CURITIBA

2008

Agradeço seus estímulos para que, desde guri, nas manhãs geladas pelo minuano, fosse em busca de um ideal.

Aos meus pais, Ivaldo Rosa e Gemma Formentini,
pela vida e pelo pão, dedico este trabalho.

AGRADECIMENTOS

Com satisfação, gostaria de agradecer o apoio de muitas pessoas que contribuíram para a realização deste estudo, direta ou indiretamente.

Inicialmente, agradeço ao Banco Central do Brasil, pela oportunidade para realização deste curso *stricto sensu*. Sou muito grato ao colega Radjalma Costa, que desde o início abriu as portas para a pesquisa, com estímulo incondicional. Aos demais colegas da autarquia que participaram da fase de campo deste estudo, inclusive com sugestões para melhorias, agradeço profundamente, omitindo seus nomes para manter a confidencialidade de dados.

A minha orientadora, Profª Ana Paula, que, do esboço inicial de delineamento do projeto às sucessivas revisões até esta versão final, constantemente acompanhou, cobrou, dirigiu e deu liberdade para que o problema de pesquisa atendesse aos requisitos prático e acadêmico.

Aos colegas pluri-regionais do curso de mestrado, pela convivência harmoniosa e enriquecedora durante todos os desafios de nossa jornada, e também por suas críticas para que versões aprimoradas do problema de pesquisa surgissem.

Ao corpo docente e servidores do Centro de Pesquisa e Pós-Graduação em Administração da UFPR, pelo profissionalismo. Aos professores Acyr Seleme, Andréa Paula Segatto-Mendes e Maria Alexandra Viegas Cortez da Cunha, pela colaboração na fase de projeto.

Aos colegas acadêmicos do BC, Antônio Francisco de Almeida Silva Jr, pela orientação técnica e freqüente incentivo; Carlos André de Melo Alves, pela contribuição na revisão teórica e problema de pesquisa; Jorge Henrique de Frias Barbosa, pelo apoio durante o curso; e Cosme Leandro do Patrocínio, por compartilhar sua experiência no tema de pesquisa.

Aos pesquisadores Gerd Van Den Eede e Rolf Von Roessing, pela cordial atenção e valiosas colaborações encaminhadas, as quais contribuíram para o embasamento teórico do trabalho.

Aos meus familiares, curitibanos e brasilienses, que com a alegria da convivência, tornaram os bons momentos desse período de intensa dedicação ao curso ainda melhor.

Aos meus jovens cientistas, Pedro (12) e André (9), por seus sorrisos que por tudo valem. Por suas virtudes na compreensão de minha ausência. À dedicada companheira que mais tempo sacrificou para que as longas horas de pesquisa se tornassem mais simples possível, Meg, todo a minha gratidão e afeto.

A Deus, pela luz que ao espírito guia.

Os problemas significativos que enfrentamos não podem ser resolvidos pelo mesmo nível de pensamento que os criou.

Albert Einstein (1879, 1955)

RESUMO

Esta é uma pesquisa multidisciplinar e multimétodos, que buscou explorar e descrever as relações entre maturidade em processos de governança de tecnologia da informação, características de organizações de alta confiabilidade e gestão de riscos operacionais em instituições financeiras. A pesquisa empírica utilizou a estratégia de estudo de caso, tendo como unidade de análise o processo de redesconto bancário conduzido na Diretoria de Política Monetária do Banco Central do Brasil. Os instrumentos de pesquisa – protocolos de entrevistas e questionário eletrônico – foram aplicados em três áreas da organização: na área de negócio, na área de tecnologia da informação e na área de auditoria interna. A análise de dados teve abordagem mista. Para a análise qualitativa, utilizou-se a análise de conteúdo e o mapa de associação de idéias. Na análise quantitativa, aplicou-se a análise de freqüências e a estatística descritiva, com apoio do teste não-paramétrico U de *Mann-Whitney*. Oito processos do modelo COBIT para governança de TI (seis processos de TI e dois processos de controle) foram selecionados para a pesquisa empírica. As conclusões evidenciam a participação desses processos na mitigação de riscos operacionais e a importância de sua gestão por níveis de maturidade para a capacitação contínua e a institucionalização desses processos de governança de tecnologia da informação. De forma complementar, constatou-se que as características de alta confiabilidade também contribuem para a mitigação de riscos operacionais, como observado nos centros de monitoramento do processo de negócio analisado. Assim, as boas práticas de governança de TI estão para a área de tecnologia da informação assim como os elementos de alta confiabilidade estão para a área de negócio. Elas são complementares entre si para a gestão de riscos operacionais.

Palavras-chave: Governança de Tecnologia da Informação; Risco Operacional; Organizações de Alta Confiabilidade; Maturidade; COBIT; Banco Central do Brasil; Redesconto Bancário; Sistema de Pagamentos Brasileiro

ABSTRACT

This is a multidiscipline and multimethod research. Its main objective was to explore and to describe the relationship among the maturity of technology information governance processes, the high reliability organizations elements and the operational risk management in financial organizations. The empirical research was conducted under a case study strategy and the unit of analyze was the discount window monetary policy instrument of Banco Central do Brasil. The research instruments – interview protocols and electronic questionnaire – were applied at three organizational areas: the business, the information technology and the audit areas. The data analysis employed mixed methods. Content analysis and ideas association maps were applied to qualitative analysis. Frequency analysis, descriptive statistical and Mann-Whitney U non-parametric test were applied to quantitative analysis. Eight processes of COBIT IT governance model (six IT processes and two control processes) were selected to the empirical research. The conclusion shows that they are important to operational risk mitigation and their maturity levels management allows the organization to evolve its skills continuously and to institutionalize these IT governance processes. Besides, the high reliability elements promote the operational risks mitigation, as it was observed at the business process monitoring centers. Thus, the IT governance best practices are to the information technology area as well as the high reliability elements are to the business area. They complement each other to the operational risk management.

Keywords: Information Technology Governance; Operational Risk**;** High Reliability Organizations; Maturity; COBIT; Banco Central do Brasil; Discount Window; Brazilian Payment System

LISTA DE QUADROS

Quadro 1 – Riscos Financeiros 23

Quadro 2 – Características dos paradigmas tecno-econômicos 36

Quadro 3 – Visão da Tecnologia da Informação nos Princípios do Basiléia II 38

Quadro 4 – Objetos de análise e variáveis relacionadas a governança corporativa 41

Quadro 5 – Tipos de Eventos de Risco no Basiléia II e sua Relação aos Aspectos de TI 49

Quadro 6 – Relevância de TI nos princípios para gestão do risco operacional 50

Quadro 7 – Cenários de TI e Objetivos de Controle 51

Quadro 8 – Princípios para aplicação de objetivos de controle 52

Quadro 9 – Processos de Governança de Tecnologia da Informação – Modelo COBIT versão 4.1 55

Quadro 10 – Sistemas Complexos *versus* Sistemas Lineares 62

Quadro 11 – Forte Acoplamento *versus* Fraco Acoplamento 62

Quadro 12 – Características de uma OAC 66

Quadro 13 – Participantes do Sistema Financeiro Nacional 67

Quadro 14 – Processos de TI selecionados para a pesquisa empírica 72

Quadro 15 – Entrevistas realizadas 87

Quadro 16 – Amostra de Respondentes por Questionário Eletrônico 88

Quadro 17 – Operações de crédito intradia (média diária) 95

Quadro 18 – Grupos de Serviços do SPB envolvidos no redesconto 97

Quadro 19 – Riscos Operacionais Tipo I - Rotina Diária 103

Quadro 20 – Riscos Operacionais Tipo II – Circunstanciais ou Hipotéticos 105

Quadro 21 – Boas Práticas em OAC – Comunicação 135

Quadro 22 – Boas Práticas em OAC – Estrutura Organizacional e Tomada de Decisão 136

Quadro 23 – Boas Práticas em OAC – Cultura 137

Quadro 24 – Boas Práticas em OAC – Aprendizagem 139

Quadro 25 – Boas Práticas em OAC e Atributos de Maturidade 141

LISTA DE FIGURAS

Figura 1 – Risco Operacional segundo Basiléia II 27

Figura 2 – Abordagens para Cálculo de Alocação de Capital para Risco Operacional 29

Figura 3 – Governança Corporativa, Gestão de Riscos e Regulamentações 32

Figura 4 – Modelo Conceitual de Organizações 33

Figura 5 – Tipologia de Tecnologia para Perrow 34

Figura 6 – Princípios de Governança Corporativa 43

Figura 7 –Controles como forma de redução de riscos 44

Figura 8 –Governança Corporativa e Governança de TI 46

Figura 9 –Governança de TI 47

Figura 10 –Foco de Atuação da Governança de TI 48

Figura 11 –Princípios Básicos do COBIT 54

Figura 12 –Modelo de Controle 57

Figura 13 –Modelos de Maturidade 58

Figura 14 – Circuitos de Aprendizagem 65

Figura 15 – Modelo conceitual proposto 75

Figura 16 – *Design* da pesquisa 89

Figura 17 – Grade Horária do STR 92

Figura 18 – Participantes do SPB 94

Figura 19 – Fluxo de mensagens da operação de redesconto 96

Figura 20 – Conformidade aos Princípios de Basiléia II 131

LISTA DE TABELAS

Tabela 1 – Avaliação e Gestão de Riscos – Distribuição de Freqüências 108

Tabela 2 – Gestão de Projetos – Distribuição de Freqüências 110

Tabela 3 – Continuidade de Serviços – Distribuição de Freqüências 111

Tabela 4 – Segurança de Sistemas – Distribuição de Freqüências 113

Tabela 5 – Gestão de RH de TI – Distribuição de Freqüências 114

Tabela 6 – Gestão de Dados – Distribuição de Freqüências 116

Tabela 7 – Estatística Descritiva da Amostra de Processos de TI 117

Tabela 8 – Cálculo das Médias de Importância dos Processos de TI, por Tipo de Risco .. 119

Tabela 9 – Teste não-paramétrico U de Mann Whitney 119

Tabela 10 – Estatística Descritiva de Maturidade de Processos de TI 127

LISTA DE GRÁFICOS

Gráfico 1 – Avaliação e Gestão de Riscos – Histograma 109

Gráfico 2 – Gestão de Projetos – Histograma 110

Gráfico 3 – Continuidade de Serviços – Histograma 112

Gráfico 4 – Segurança de Sistemas – Histograma 113

Gráfico 5 – Gestão de RH de TI – Histograma 115

Gráfico 6 – Gestão de Dados – Histograma 116

Gráfico 7 – Distribuição Normal de Maturidade 130

LISTA DE ABREVIATURAS

BCB	Banco Central do Brasil
BIS	Bank for International Settlements
CGU	Controladoria Geral da União
CMM	*Capability Maturity Model*
COBIT	*Control Objectives for Information and related Technology*
COSO	Committee of Sponsoring Organizations
DC	Definição Constitutiva de Variável ou Constructo
DEAUB	Departamento de Auditoria Interna
DEBAN	Departamento de Operações Bancárias e Sistemas de Pagamentos
DEINF	Departamento de Tecnologia da Informação
DEMAB	Departamento de Operações de Mercado Aberto
DIPOM	Diretoria de Política Monetária
DO	Definição Operacional de Variável ou Constructo
DVP	*Delivey Versus Payment*
ERM	*Enterprise Risk Management*
ISO	International Organisation for Standardisation
ITGI	Information Technology Governance Institute
ITIL	*IT Infrastructure Library*
OAC	Organizações de Alta Confiabilidade
OCDE	Organização para Cooperação e Desenvolvimento Econômico
P&D	Pesquisa e Desenvolvimento
PMI	Project Management Institute
PU	Preço unitário
Quest	Questionário
RDC	Redesconto

Resp	Respondente
RSFN	Rede do Sistema Financeiro Nacional
SEI	Software Engineering Institute
SELIC	Sistema Especial de Liquidação e de Custódia
SFN	Sistema Financeiro Nacional
SOX	Lei Sarbanes-Oxley
SPB	Sistema de Pagamentos Brasileiro
SPC	Secretaria de Previdência Complementar
SPSS	Statistical Package for the Social Sciences
STR	Sistema de Transferência de Reservas
SUSEP	Superintendência de Seguros Privados
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
TIC	Tecnologias de Informação e Comunicação

SUMÁRIO

1 INTRODUÇÃO 16

1.1 Formulação do Problema 18

1.2 Objetivos 18

1.3 Relevância do Tema 19

1.4 Justificativa Teórica e Prática 20

1.5 Estrutura da Dissertação 21

2 REFERENCIAL TEÓRICO-EMPÍRICO 22

2.1 Risco Operacional 23

2.1.1 Risco, Incerteza e Mitigação 24

2.1.2 O Novo Acordo da Basiléia 24

2.1.3 Risco Operacional : a Inovação no Basiléia II 26

2.1.4 Pilares do Acordo da Basiléia II 28

2.1.5 Aspectos Qualitativos do Risco Operacional 30

2.2 Tecnologia da Informação e Comunicação 32

2.2.1 Tecnologia e Organização 33

2.2.2 O Paradigma da Tecnologia da Informação 35

2.2.3 O Componente de Tecnologia da Informação no Risco Operacional 37

2.3 Governança Corporativa e de Tecnologia da Informação 40

2.3.1 Governança Corporativa, Gestão de Riscos e Controle Interno 40

2.3.2 Governança de Tecnologia da Informação 46

2.3.3 Análise de Cenários e Objetivos de Controle para TI 49

2.3.4 Modelo COBIT para Governança de TI 53

2.3.5 Gestão de Processos por Níveis de Maturidade 57

2.4 Organizações de Alta Confiabilidade - OAC 60

2.4.1 Características 61

2.4.2 Sistema Financeiro Nacional 67

3 METODOLOGIA 71

3.1 Especificação do Problema 71

3.1.1 Perguntas de Pesquisa 71

3.1.2 Modelo Conceitual 72

3.1.3 Definição Constitutiva e Operacional das Variáveis 76

3.1.4 Definição de Outros Termos Relevantes 82
3.2 Delimitação e *Design* da Pesquisa 83
3.2.1 Delineamento da Pesquisa 83
3.2.2 População e Amostra 85
3.2.3 Dados: Coleta e Tratamento 86
4 APRESENTAÇÃO E ANÁLISE DOS DADOS 90
4.1 Redesconto Bancário 90
4.1.1 Descrição do Processo 90
4.1.2 Operacionalização do Processo de Redesconto 96
4.1.3 Riscos Operacionais no Processo de Redesconto 99
4.2 Processos de Governança de Tecnologia da Informação 107
4.2.1 Avaliação e Gestão de Riscos 108
4.2.2 Gestão de Projetos 110
4.2.3 Continuidade de Serviços 111
4.2.4 Segurança de Sistemas 113
4.2.5 Gestão de RH de TI 114
4.2.6 Gestão de Dados 116
4.2.7 Estatística Descritiva dos Processos 117
4.3 Processos de Controle Governança de Tecnologia da Informação 120
4.3.1 Promoção de Governança de TI 121
4.3.2 Avaliação e Monitoramento de Controles Internos 123
4.4 Maturidade de Processos e Aplicabilidade para Gestão 126
4.5 Alta Confiabilidade 132
4.5.1 Tipologia de Alta Confiabilidade 132
4.5.2 Boas Práticas de Alta Confiabilidade 134
5 CONSIDERAÇÕES FINAIS 147
REFERÊNCIAS BIBLIOGRÁFICAS 154
ANEXO A – NÍVEIS DE MATURIDADE DE PROCESSOS 164
ANEXO B – PROTOCOLO DE ENTREVISTA: Descrição do Processo de Negócio .. 171
ANEXO C – PROTOCOLO DE ENTREVISTA: Riscos Operacionais 172
ANEXO D – PROTOCOLO DE ENTREVISTA: Processos de Controle 173
ANEXO E – PROTOCOLO DE ENTREVISTA: Alta Confiabilidade 174
ANEXO F – QUESTIONÁRIO ELETRÔNICO: Processos de TI e Maturidades 176

1 INTRODUÇÃO

Desde a antiguidade, os seres humanos buscam meios de antever os acontecimentos do futuro. As antigas civilizações gregas e romanas atribuíam esse poder a seus deuses, como Tirésias e Fortuna. Nessas culturas tradicionais, o livre arbítrio não se constituía em atributo compartilhado. Dominante naquela época, o pensamento mítico excluía outras perspectivas de explicação dos acontecimentos naturais. De cunho determinista, a natureza humana não contemplava a possibilidade de arriscar-se.

No século VI a.C., a forma de conceber o mundo é alterada paulatinamente, fruto de um movimento de secularização da sociedade e do surgimento de cidades-Estado. Com berço na Grécia antiga, a ciência surge com o início do pensamento filosófico-científico, abrindo espaço para a discussão do mito e transformação na sociedade. Os filósofos da escola jônica, dando início ao processo de geração de conhecimento baseado em causas naturais, que constituiu a escola naturalista, buscavam a explicação do mundo no próprio mundo, e não fora dele (MARCONDES, 2005).

A racionalidade nas decisões é destacada por Bernstein (1997, p.1), para quem "a idéia revolucionária que define a fronteira entre os tempos modernos e o passado é o domínio do risco: a noção de que o futuro é mais do que um capricho dos deuses e de que homens e mulheres não são passivos ante a natureza". Derivada do latim *risicu* e do italiano antigo *risicare*, a palavra risco traz consigo o signo ousadia (BERNSTEIN, 1997).

O risco é inerente à atividade financeira. Desde a intermediação até o processamento operacional, falhas, incorreções processuais e desvirtuamento de interesses podem acarretar prejuízos a uma das partes e ao sistema como um todo.

As organizações participantes do Sistema Financeiro Nacional (SFN), tanto no subsistema de intermediação de recursos entre agentes econômicos quanto no subsistema normativo, desenvolvem processos de negócio para cumprirem seus objetivos estratégicos. No desempenho desses processos, tais organizações – aqui definidas como instituições financeiras – ficam expostas a riscos financeiros, como os riscos de crédito, de mercado, sistêmico e operacional.

Este último, o risco operacional, refere-se à possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos (BIS, 2004, p.137; BACEN, 2006, p.1).

No Brasil, a regulação e normatização do sistema financeiro são de responsabilidade do Banco Central do Brasil. A relevância de sua atuação para estabilidade na intermediação financeira, sua abrangência e complexidade e o reduzido índice de erros verificado o caracterizam como organização de alta confiabilidade .

Atuando no subsistema normativo do SFN, o Banco Central do Brasil (BCB), seguindo recomendações de boas práticas de governança corporativa do Banco de Compensações Internacionais (Bank for International Settlements – BIS), publicou a Resolução nº 3.380, que versa sobre a obrigatoriedade da implementação de estrutura de gerenciamento de risco operacional nas instituições financeiras.

Exercendo outra função típica de bancos centrais, o BCB é responsável pela execução da política monetária, que envolve a administração do sistema de pagamentos brasileiro, a gestão das reservas internacionais e as operações de mercado aberto. Em suas atividades, a autoridade monetária também incorre em riscos operacionais.

O risco operacional apresenta um importante componente constitutivo: a tecnologia da informação e comunicação. Desta forma, estruturas de governança corporativa para gestão de risco devem ser integradas e estendidas por estruturas de governança de tecnologia da informação para o controle e mitigação de riscos operacionais, em que os níveis de maturidade na capacitação de seus processos são importantes indicadores da adoção de boas práticas.

As abordagens para alocação de capital adotadas pelas instituições financeiras, para resguardar possíveis perdas advindas do risco operacional, prevêem aspectos quantitativos e qualitativos. Dentre os critérios qualitativos, encontram-se a análise de cenários, controles internos e boas práticas para gestão e supervisão do risco operacional.

Organizações de alta confiabilidade, tipologia que inclui os bancos e outras organizações que atuam em um contexto de alto risco, possuem características como

comunicação, cultura e estrutura organizacional que lhes fornecem confiabilidade e flexibilidade de operações. Estas características são importantes para a maturidade de processos de tecnologia da informação.

Diante deste panorama, formula-se o problema de pesquisa a seguir descrito.

1.1 Formulação do Problema

A elaboração do problema de pesquisa considerou a interdisciplinaridade do contexto anteriormente apresentado. O propósito deste trabalho foi explorar os aspectos qualitativos de boas práticas para gestão do risco operacional em instituições financeiras, por meio da investigação da maturidade de processos de governança de tecnologia da informação em um ambiente considerado de alta confiabilidade.

A seguinte questão de pesquisa foi investigada:

COMO A MATURIDADE NOS PROCESSOS DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO E AS CARACTERÍSTICAS DE ALTA CONFIABILIDADE CONTRIBUEM PARA A MITIGAÇÃO DO RISCO OPERACIONAL EM INSTITUIÇÕES FINANCEIRAS?

1.2 Objetivos

O objetivo geral deste estudo é investigar aspectos qualitativos para a gestão de riscos operacionais em instituições financeiras, analisando a maturidade de processos de um modelo de governança de tecnologia da informação e também características pressupostas de alta confiabilidade operacional. Para alcançar esse objetivo, foi selecionado um processo de negócio no Banco Central do Brasil para estudo de caso, e os seguintes objetivos específicos são desenvolvidos:

1. Identificar os riscos operacionais envolvidos no processo de negócio selecionado;

2. Verificar o grau de contribuição dos processos de governança de tecnologia da informação para a mitigação dos riscos operacionais identificados;

3. Analisar a importância dos processos de controle de governança de tecnologia da informação;

4. Investigar a aplicabilidade de modelos de maturidade para a gestão de processos; e

5. Propor novos fatores de maturidade para governança de TI, em função das características de alta confiabilidade percebidas;

1.3 Relevância do Tema

Segundo Marshall (2002, p.3), "em uma pesquisa recente realizada pela PricewaterCoopers e pela British Bankers Association, aproximadamente 70 por cento dos bancos no Reino Unido consideravam seus riscos operacionais tão importantes quanto seus riscos de mercado ou de crédito."

As mudanças ocorridas ao longo das últimas décadas, principalmente após o surgimento das tecnologias de informação e comunicação (TIC) e sua constante evolução, bem como a transformação dos mercados e a sofisticação dos produtos financeiros, trouxeram implicações diretas para o *modus operandi* no setor financeiro e para sua fiscalização.

Carneiro *et al.* (2006) salientam que a indústria bancária tem crescentemente demandado pesquisas em sua área, uma vez que tem importante papel no desenvolvimento social e econômico de um país, sendo, ainda, fonte de preocupação constante de poupadores e tomadores de recursos, além dos órgãos reguladores e instituições governamentais. Assim, estudos acadêmicos na área de gestão de riscos financeiros contribuem para o aperfeiçoamento da gestão bancária, cujo interesse é do Sistema Financeiro Nacional como um todo.

Os eventos históricos de perdas resultantes da exposição ao risco operacional, coletados por Marshall (2002 p.21), evidenciam o volume financeiro afetado e a conseqüente importância do aprofundamento de pesquisas para o acompanhamento e controle deste tipo de risco. No Brasil, as instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central, atendendo à Resolução nº 3.380 da autoridade monetária (BACEN, 2006), estão em processo de implementação de estrutura para gerenciamento do risco operacional, o que torna o estudo do risco operacional relevante para estas organizações.

1.4 Justificativa Teórica e Prática

A motivação para este estudo científico deve-se ao fato de que as pesquisas acerca de gerenciamento de riscos, de uma maneira geral, são difundidas no meio acadêmico, porém há carência de contribuições empíricas sobre a administração de risco operacional, que é uma concepção relativamente mais nova do que outros riscos, como o risco de crédito e o risco de mercado.

Atualmente as instituições financeiras têm se deparado com desafios práticos para a implementação de uma estrutura organizacional para a administração do risco operacional, que foi uma das principais recomendações do Novo Acordo da Basiléia, divulgado em junho de 2004, e que foi normatizada pelo BCB para implementação por essas instituições até o final do ano de 2007.

Outra motivação prática para este trabalho relaciona-se com os estudos de gerenciamento de riscos em bancos centrais, que são entidades de alta confiabilidade em virtude de sua inserção no sistema financeiro nacional.

Meirelles *et al.* (2005) salientam a importância de se assegurar sistemas de governança adequados para as autoridades monetárias, com a finalidade de garantir a estabilidade das economias nacionais, dos sistemas financeiros domésticos e, conseqüentemente, mundiais. Meirelles *et al.* (2005, p.1) avaliam que

> partindo do pressuposto de que os bancos centrais têm um papel fundamental na regulação e supervisão do sistema financeiro, e que, também, estão expostos a riscos, chega-se ao entendimento de que essas autoridades supervisoras devem assumir uma postura de *liderança pelo exemplo* e, assim,

> precisam também adotar políticas de gestão de riscos que ampliem sua governança corporativa.

Guldentops *et al.*(2002) e Gerke e Ridley (2006) realizaram estudos que apontam para o potencial de utilização do modelo COBIT para governança de tecnologia da informação (TI). A validação desse modelo no cenário brasileiro e a investigação da importância de seus processos para a mitigação do risco operacional é uma contribuição para as pesquisas nessa área de conhecimento.

Delimitando o estudo do risco operacional em seu componente de tecnologia da informação, este estudo visa contribuir com evidências empíricas sobre a contribuição da governança de TI e a aplicabilidade de modelos de maturidade para a gestão de seus processos. Santos (2003) analisa os modelos de gestão por processos e gestão por níveis de maturidade, e conclui que a convergência entre ambos vai ao encontro de um modelo inovador de gestão, por possibilitar a análise da melhoria contínua de processos organizacionais.

De forma complementar, busca-se também a validação das características de alta confiabilidade, pressupostas para uma organização pertencente a esta tipologia, as quais concorrem para a mitigação de riscos operacionais, conforme Eede e Walle (2005), Pinto (2005) , Eede *et al.* (2006).

1.5 Estrutura da Dissertação

A estrutura deste documento é composta por cinco capítulos, seguidos pelos referenciais bibliográficos adotados e anexos da pesquisa.

O primeiro capítulo destina-se à apresentação do tema, sua relevância e formulação do problema de pesquisa, bem como do objetivo geral e objetivos específicos do estudo, e sua justificação teórica e prática.

No segundo capítulo é construído o arcabouço teórico-empírico que constitui o referencial para a elaboração do modelo conceitual da investigação. Discorre-se acerca de

quatro grandes tópicos: (i) Risco Operacional; (ii) Tecnologia da Informação e Comunicação; (iii) Governança de Tecnologia da Informação; e (iv) Organizações de Alta Confiabilidade.

O terceiro capítulo tem por finalidade elucidar a metodologia científica adotada. O problema de pesquisa é referenciado e são apresentadas as perguntas de pesquisa. Apresenta-se o modelo conceitual com relações multivariadas e as definições constitutivas e operacionais das variáveis. Faz-se, em seguida, o delineamento da pesquisa, apresentando a estratégia de estudo de caso único, realizado no processo de negócio de Redesconto Bancário conduzido pela Diretoria de Política Monetária do Banco Central do Brasil. As atividades de campo são descritas e é apresentado o *design* geral para coleta e tratamento de dados.

O capítulo número quatro destina-se à apresentação e análise dos dados. O processo de Redesconto Bancário é descrito, bem como sua operacionalização e riscos operacionais identificados. Em seguida, é investigada a importância da maturidade dos processos de tecnologia da informação e dos processos de controle para a mitigação dos riscos operacionais, e as características de alta confiabilidade são validadas.

O quinto capítulo traz as considerações finais, à luz das evidências empíricas constatadas. As perguntas de pesquisa são retomadas, e estudos futuros são sugeridos, bem como são apresentadas as limitações deste estudo.

2 REFERENCIAL TEÓRICO-EMPÍRICO

A revisão da literatura pertinente ao escopo desta pesquisa abrange o novo Acordo da Basiléia (Basiléia II) em seu enfoque de risco operacional; o paradigma das tecnologias de informação e comunicação; a governança de tecnologia da informação; e as organizações de alta confiabilidade.

2.1 Risco Operacional

Este item do referencial teórico-empírico discorre acerca do risco operacional, que ao lado de outros riscos financeiros, passou a figurar nas recomendações do Comitê da Basiléia, detalhado adiante.

O Quadro 1 traz a tipologia de riscos financeiros.

Quadro 1 – Riscos Financeiros

Tipo	Descrição
Risco de crédito	Risco decorrente da possibilidade de que a contraparte não honre a entrega de papéis ou fundos pactuados, não liquidando uma obrigação por seu valor completo, seja no vencimento ou em qualquer oportunidade a partir desse momento
Risco de mercado	Risco de perdas nas posições de balanço e extra-balanço devido a movimentos (volatilidades) nos preços de mercado dos ativos
Risco legal	Refere-se tanto à falta de uma legislação mais atualizada e eficiente com relação ao mercado financeiro como a um eventual desconhecimento jurídico na realização dos negócios
Risco de liquidez	Risco de indisponibilidade imediata de caixa diante de demandas por parte dos depositantes e aplicadores de uma instituição financeira. Pode surgir em função do volume de negócios e instabilidade das condições de mercado
Risco sistêmico	Risco de que a inadimplência de um participante possa fazer com que outros participantes, por sua vez, não consigam cumprir suas obrigações no vencimento
Risco de câmbio	Risco relacionado à desvalorização ou valorização cambial da moeda nacional em relação a moedas estrangeiras, dependendo da posição comprada ou vendida de investimentos no exterior
Risco soberano	Risco relacionado à regularidade de fluxos de pagamentos externos e até mesmo a decretação de moratória de dívidas. Não há tribunais internacionais competentes para julgar pedidos de falência de um país
Risco operacional	Possibilidade de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos

Fonte: BACEN (2007c, p. 49-50), BACEN (2006, p.1), Assaf Neto (2005, p. 97-99)

Antes de enfocar o risco operacional especificamente, a seguir são introduzidos os conceitos de risco, incerteza e mitigação.

2.1.1 Risco, Incerteza e Mitigação

Marshall (2002, p.37) observa a distinção entre risco e incerteza. “Risco se aplica a resultados que, embora não certos, tenham probabilidades que possam ser estimadas pela experiência ou dados estatísticos. A incerteza está presente quando o resultado não pode ser previsto, nem mesmo em um sentido probabilístico”. Ou seja, a diferenciação entre ambos está na previsibilidade dos resultados ou diminuição de sua aleatoriedade.

Marshall (2002) descreve as diferentes dimensões para a conceituação de risco: (i) risco como resultado médio, utilizado no campo das ciências atuariais, denota o risco como sendo o resultado esperado; (ii) risco como variância de resultado, mais utilizado no campo das finanças, refere-se ao desvio-padrão dos resultados observados; (iii) risco como fator catastrófico negativo, utilizado em controles internos, planejamento de contingências e auditorias, traz uma visão mais defensiva de risco e o considera como sendo um perigo a ser minimizado; e (iv) risco como fator positivo de oportunidade, que é assumido e gerenciado para possibilitar retornos futuros.

Bernstein (1997, p.8) salienta que “risco é uma opção, e não um destino”. Por isso, os riscos podem ser assumidos, evitados ou mitigados. A mitigação consiste na alocação, controle, compartilhamento ou financiamento do risco (BERGAMINI JR, 2005). Mitigar significa reduzir para um nível aceitável as conseqüências ou probabilidade de um evento de risco adverso (PMBOK, 2000).

Neste trabalho, é considerada a terceira dimensão conceitual de risco, qual seja, um fator negativo a ser minimizado por meio de sua mitigação via controle.

2.1.2 O Novo Acordo da Basiléia

Fundado em 1930, o Banco de Compensações Internacionais (BIS), conhecido como o banco central dos bancos centrais, vem elaborando, por meio de um comitê de supervisão bancária, recomendações de práticas de governança corporativa para organizações bancárias

internacionais e para os respectivos órgãos de regulação e de supervisão, com o objetivo de fortalecer a estabilidade financeira mundial (MEIRELLES *et al.*, 2005).

O Comitê de Supervisão Bancária da Basiléia foi criado em 1974, por um grupo de bancos centrais de países desenvolvidos, o chamado Grupo dos 10. Atualmente as suas reuniões são trimestrais, com participação de representantes da Alemanha, Bélgica, Canadá, Estados Unidos, França, Holanda, Itália, Japão, Luxemburgo, Reino Unido, Suécia e Suíça (GONÇALVEZ, 2007). O seu objetivo principal é formular políticas supranacionais de supervisão bancária, com recomendações de controle interno, governança corporativa e supervisão bancária. Contudo, o Comitê não possui autoridade formal.

Uma de suas principais diretrizes foi a abordagem do capital regulatório para cobrir perdas eventuais inerentes a riscos assumidos por bancos, prevenindo, assim, o risco sistêmico, em que uma falha financeira em uma instituição pode contaminar outras instituições, em razão da forte interdependência de recursos monetários existente entre elas, gerando um "efeito dominó".

Em 1988, o Comitê elaborou o Acordo da Basiléia, que trazia recomendações às instituições financeiras para a alocação de capital mínimo como forma de prevenção para que eventuais perdas monetárias, relativas à sua exposição ao risco de crédito, não afetassem a solidez institucional e, conseqüentemente, sistêmica. Posteriormente, em 1996, tal Comitê reforçou as medidas recomendáveis para a estabilidade financeira ao emendar o Acordo da Basiléia com a publicação do "*Amendment to the Capital Accord to Incorporate Market Risks*", que incorporava metodologia para consideração do risco de mercado (MEIRELLES *et al*., 2005; COIMBRA, 2006).

Por último, em junho de 2004, o Comitê, após consultas públicas a entidades financeiras, e com participação dos bancos centrais, principalmente dos países do G-10, apresentou o documento "Convergência Internacional de Mensuração e Padrões de Capital: Uma Estrutura Revisada", que passou a ser referenciado como Basiléia II (BIS, 2004; MEIRELLES *et al.*, 2005; ALVES, 2005; COIMBRA, 2006).

O Basiléia II representa uma das mais significativas mudanças de regulamentação no setor financeiro nas últimas décadas. As atividades para sua implementação iniciaram em 2006 e para os países do G-10 têm previsão para conclusão em 2008.

2.1.3 Risco Operacional : a Inovação no Basiléia II

Marshall (2002, p.21) observa que, segundo uma pesquisa realizada pela Operational Risk Inc., "desde 1980 instituições financeiras têm perdido mais de US$ 200 bilhões devido a riscos operacionais". Recentemente, em janeiro de 2008, a fraude de cerca de US$ 7 bilhões no banco francês Société Générale, causada por um único operador, reforçou a necessidade de maior controle do risco operacional.

Nesse sentido, Eede e Walle (2005) e Bergamini Jr (2005) retratam casos famosos de falhas operacionais em empresas como Banco Barings[1] (1995) e Enron (2002) e perdas de bilhões de dólares com a quebra do fundo de derivativos Long Term Capital Management (1998). Tais eventos contribuíram para uma alteração da ênfase tradicional com foco em riscos comerciais para o processo de gestão de riscos operacionais. Este contexto levou o Congresso dos Estados Unidos a editar a Lei Sarbanes-Oxley (SARBANES-OXLEY, 2002), para promover os princípios de governança corporativa nas empresas americanas ligadas ao mercado de capitais, reescrevendo as regras para divulgação e emissão de relatórios financeiros.

Desta forma, a Lei Sarbanes-Oxley (SOX) aumenta a responsabilidade dos executivos e intensifica as medidas para conferências e controles internos. Enquanto que a SOX determina a gestão do risco operacional em geral, o acordo da Basiléia II dá maior ênfase aos esforços para controle de riscos operacionais especificamente em instituições financeiras.

Assim, o Basiléia II agregou o componente operacional ao processo de gerenciamento de riscos em instituições financeiras, que já atendia aos requisitos de exigência de alocação de capital para riscos de crédito e de mercado.

---

[1] A história do operador Nick Leeson, gerente geral que acumulava funções de controle e na mesa de operações do banco, atuando no mercado de derivativos da Bolsa de Cingapura, é exibida em filme (A FRAUDE, 1999).

Dentre as definições para risco operacional (ALVES, 2005; COIMBRA, 2006), a de maior aceitação nos estudos acadêmicos é a fornecida pelo Basiléia II e difundida no sistema financeiro nacional pelos órgãos reguladores, a exemplo do Banco Central do Brasil, que em sua Resolução nº 3.380 dispõe sobre a implementação de estrutura de gerenciamento de risco operacional. Esta definição conceitua risco operacional como "a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos." (BIS, 2004, p.137; BACEN, 2006, p.1).

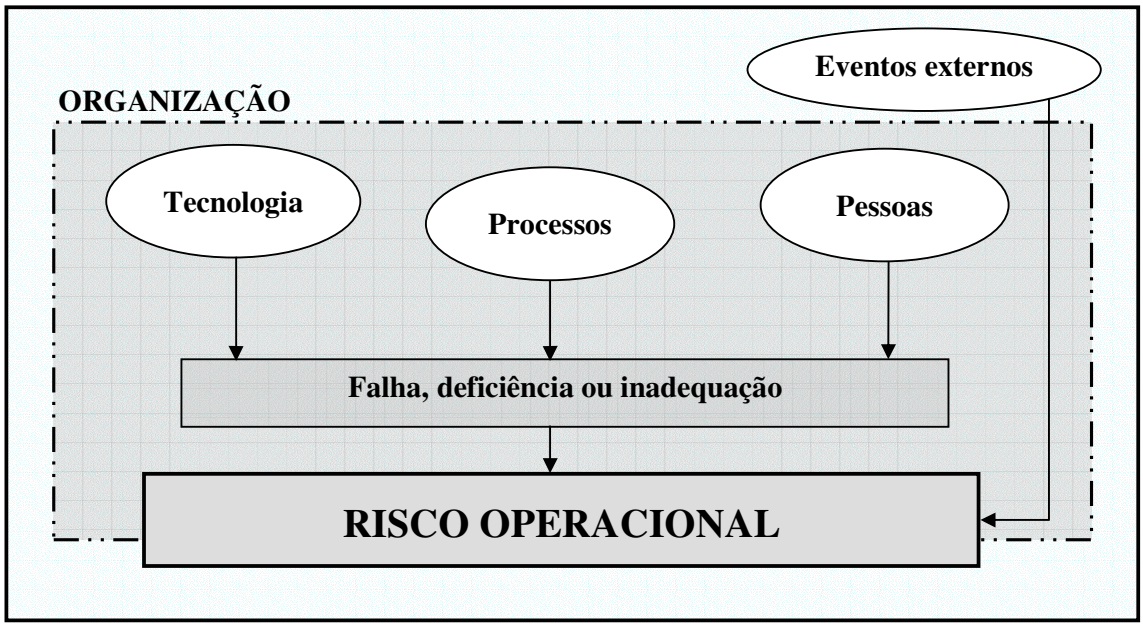


Figura 1 – Risco Operacional segundo Basiléia II
Fonte: O autor, a partir de BIS, 2004, p. 137

O risco operacional tem natureza assimétrica, pois à exposição a este tipo de risco não se relaciona, diretamente, algum retorno, diz Bergamini Jr (2005). Para ele, é difícil observar um padrão de recorrência de riscos operacionais, o que dificulta o uso de medidas estatísticas com base na distribuição de freqüências.

O risco operacional será transformado de uma referência obscura em uma fundamental consideração de negócio, porquanto o Basiléia II será o condutor-chave para inovações no setor financeiro, assim como a SOX está sendo para as demais organizações em seu relacionamento com *stakeholders*, como observam Eede e Walle (2005). Os *stakeholders* são

indivíduos ou grupos afetados por danos e benefícios reais ou potenciais resultantes da ação ou inação da organização. Quando o seu suporte é vital para a existência da organização, eles são considerados *stakeholders* estratégicos (TURNBULL, 1997).

2.1.4 Pilares do Acordo da Basiléia II

As atuais recomendações do Comitê da Basiléia têm como base três linhas de atuação. Além das observações relativas à exigência de alocação de capital para fazer frente à probabilidade de perdas, o Basiléia II sugere a supervisão bancária e também a maior transparência das instituições financeiras como formas de controle de riscos (BIS, 2004).

Ou seja, são três os pilares de sustentação do Basiléia II:

1. Exigência de capital prudencial mínimo, compatível com a exposição aos riscos de crédito, de mercado e operacional das instituições financeiras;
2. Atuação dos órgãos supervisores no processo de solidez do sistema financeiro, que devem assegurar a adequação do capital alocado por parte dos bancos, e intervir se necessário; e
3. Transparência e disciplina de mercado no processo de divulgação de informações aos *stakeholders*;

Além de metodologias para cálculo de alocação de capital para risco de crédito e de mercado, o primeiro pilar do acordo apresenta também três abordagens relacionadas ao risco operacional, em um *continuum* de crescente sofisticação e sensibilidade ao risco: Método Básico; Método Padronizado; e Métodos Avançados (BIS, 2004). As instituições financeiras são estimuladas a desenvolver práticas e sistemas de gestão de risco operacional cada vez mais elaborados, que tendem a gerar menor alocação de capital e, por conseqüência, maior vantagem competitiva no mercado. O uso do Método Padronizado e de Métodos Avançados está sujeito à aprovação de órgão supervisor, após seu monitoramento e validação por um período inicial (BIS, 2004). A Figura 2 exibe os métodos para cálculo de capital para risco operacional apresentados no Basiléia II.

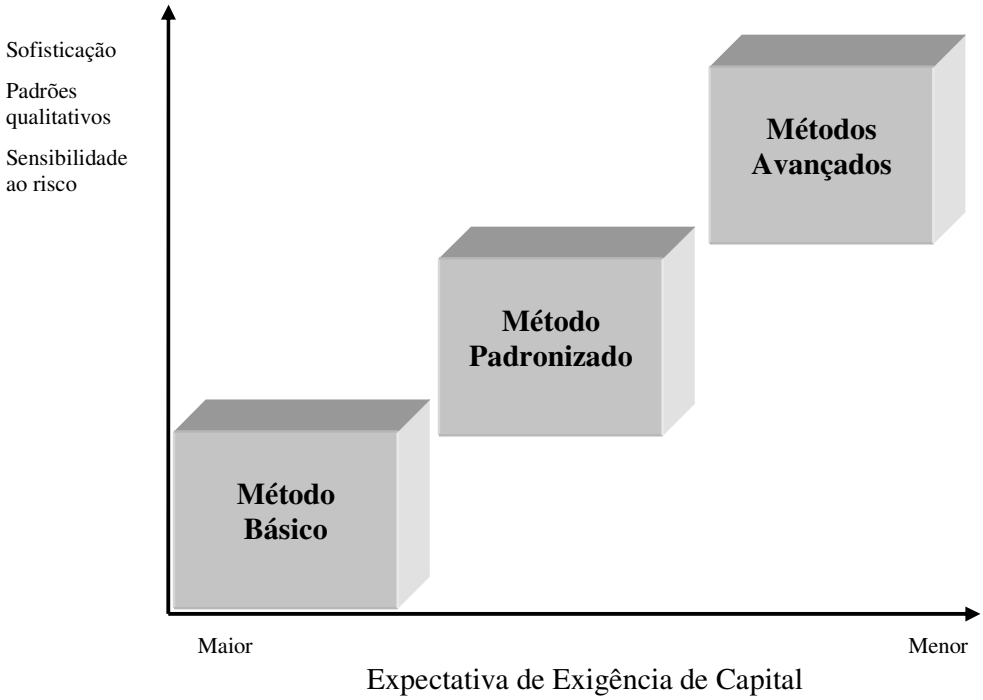


Figura 2 – Abordagens para Cálculo de Alocação de Capital para Risco Operacional (Adaptado de ITGI, 2007, p. 18).

Para a qualificação ao uso dos Métodos Padronizado e Avançado são especificados critérios qualitativos mínimos que devem ser alcançados pelos bancos. O ponto de entrada para o cálculo, o Método Básico, não prevê tais critérios, porém as instituições financeiras que usarem esta abordagem são estimuladas a seguir as recomendações reunidas no documento "*Sound Practices for the Management and Supervision of Operational Risk*" (BIS,2003).

Comuns aos Métodos Padronizado e Avançado, são especificados os seguintes critérios: (i) o conselho de administração e a gerência sênior devem estar ativamente envolvidos na definição de uma estrutura para gestão do risco operacional; (ii) deve haver um sistema de gestão do risco operacional que seja conceitualmente válido e implementado com integridade; e (iii) deve haver recursos suficientes para atuação nas principais áreas de negócio assim como nas áreas de auditoria e controle. A adequação a esses critérios é verificada pelos órgãos supervisores bancários.

Especificamente para os Métodos Avançados, a metodologia de avaliação de risco desenvolvida pelo banco deve, ainda, estimar as perdas inesperadas com base na combinação

de dados internos e de dados externos relevantes de perdas, análise de cenários e fatores dos ambientes específicos de negócio e de controles internos que podem alterar o perfil de risco.

Conforme o acordo (BIS, 2004, p. 147),

> estes fatores [de controle interno] tornarão as avaliações de risco dos bancos mais progressivas, refletindo mais diretamente a qualidade de controle e ambiente de operações do banco, auxiliando a avaliação de capital com objetivos de gerenciamento de risco, e reconhecendo tanto as melhorias quanto as deteriorações nos perfis de risco operacional, de uma maneira mais imediata.

O ITGI (2007) argumenta que a adequação de capital, com base nos modelos quantitativos de ativos ponderados pelo risco, não é suficiente para trazer estabilidade aos mercados financeiros. O desenvolvimento de sistemas de gerenciamento de riscos, com aplicação de sistemas de controle de riscos internos, pode diminuir a necessidade de alocação de capital.

Aplicando esta filosofia, os órgãos de supervisão – que compõem o segundo pilar – estarão privilegiando os modelos com características mais qualitativas de supervisão bancária.

2.1.5 Aspectos Qualitativos do Risco Operacional

Marshall (2002) observa a contribuição das iniciativas de órgãos reguladores e setoriais na elaboração de padrões quantitativos e qualitativos para a gerência do risco operacional, mencionando os seguintes padrões qualitativos: diretrizes de controle interno; diretrizes setoriais de boas práticas operacionais; e diretrizes de qualidade para processos e recursos.

Complementares entre si, as ações para reforçar os sistemas de controle interno, as boas práticas para gestão de risco e para governança corporativa têm como destaque:

- a Lei Sarbanes-Oxley (SARBANEX-OXLEY, 2002), especificamente em sua Seção 404, que trata de controles internos;

- as publicações do Committee of Sponsoring Organizations (COSO[2]), em sua estrutura para integração de controles internos e estrutura integrada para gestão de risco na empresa (*Enterprise Risk Management – ERM)*;

- as recomendações do Comitê da Basiléia para Supervisão Bancária, como o "*Framework for the Evaluation of Internal Control Systems"* (BIS, 1998) e o "*Sound Practices for the Management and Supervision of Operational Risk*" (BIS, 2003);

- as publicações do Information Technology Governance Institute (ITGI), como o "*Control Objectives for Information and related Technology – CobiT"* (ITGI, 2005); o "*IT Control Objectives for Sarbanes-Oxley"* (ITGI, 2006); e o "*IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance – Exposure Draft"* (ITGI ,2007).

Segundo o ITGI (2007), o *framework* definido pelo COSO é um dos mais utilizados para a gestão de riscos e para controles internos nos bancos, especialmente naqueles que devem cumprir as determinações da Lei Sarbanes-Oxley (SOX). Essa estrutura, representada na Figura 3, abrange aspectos de governança corporativa, gestão de riscos e *compliance* ou conformidade, que é uma função exercida nos sistemas de controle interno, com o objetivo de verificar se as regulamentações legais aplicáveis nas atividades da organização estão sendo cumpridas, evitando perdas financeiras ou baixas de reputação para a instituição (ALVES, 2005b).

[2] COSO, organização privada dos EUA, é composto pelo Americam Institute of Certified Public Accountants, Americam Accouting Association, Financial Executives International, Institute of Internal Auditors e Institute of Management Accountants.

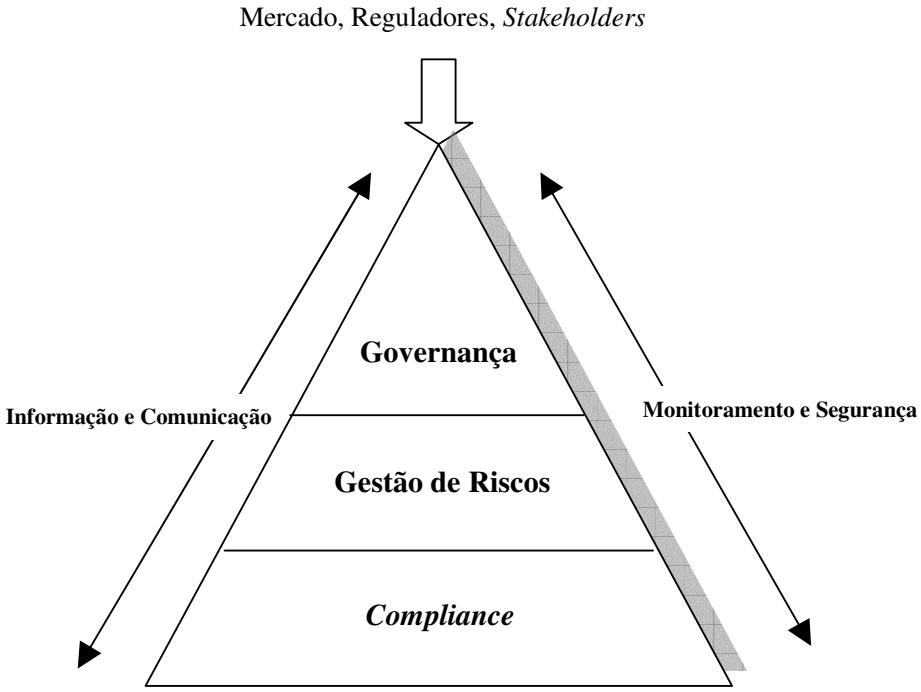


Figura 3 – Governança Corporativa, Gestão de Riscos e Regulamentações (Adaptado de ITGI, 2007, p. 11).

Desta forma, a estrutura do COSO constitui-se em uma base agregada para planejamento, projeto e implementação de gerenciamento de riscos nas organizações, cobrindo aspectos de auditoria financeira (SOX) e de risco operacional (Basiléia II).

Entretanto, "sua estrutura para gestão de riscos na empresa não abrange especificamente a gestão de informação e a tecnologia da informação" (ITGI, 2007, p.22).

2.2 Tecnologia da Informação e Comunicação

Este segundo tópico do referencial teórico-empírico aborda o paradigma da tecnologia da informação e comunicação e sua importância no contexto do Basiléia II.

2.2.1 Tecnologia e Organização

Hatch (1997) apresenta o modelo de cinco círculos, em que representa as organizações como um conjunto de tecnologias, estruturas sociais, culturas e estruturas físicas, em que as relações estão sobrepostas entre si, inseridas em um contexto ambiental.

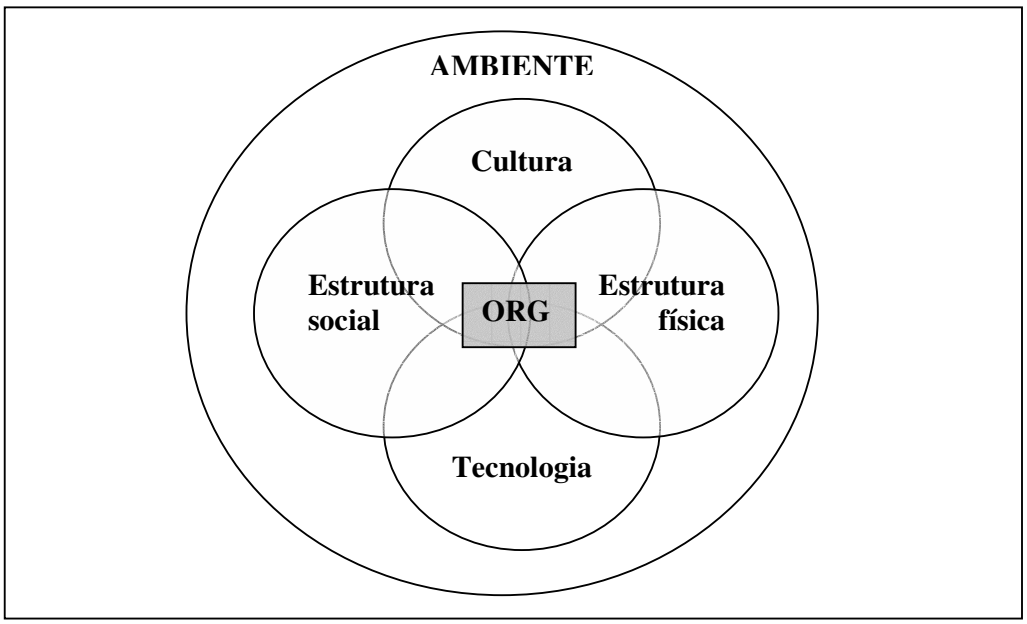


Figura 4 – Modelo Conceitual de Organizações (Hatch, 1997, p. 15).

O conceito de tecnologia está relacionado aos meios para se alcançar algum fim – um resultado desejado, um objetivo, um produto ou serviço. Nesta perspectiva, Hatch (1997) define tecnologia como: (1) objetos físicos ou artefatos, incluindo produtos e ferramentas, e equipamentos usados na sua produção; (2) atividades ou processos que constituem os métodos de produção; e (3) o conhecimento necessário para desenvolver e aplicar em equipamentos, ferramentas e métodos para produzir um resultado particular.

Roberts e Grabowski (1996, p.316) classificam as tecnologias em mecânicas, humanas e de conhecimento:

> As *tecnologias mecânicas* referem-se a máquinas, ferramentas e equipamentos usados na produção de bens (...). As *tecnologias humanas* consistem nas habilidades e na energia física usadas na produção de bens e

> podem ser substituídas por tecnologias mecânicas. As *tecnologias de conhecimento* referem-se aos significados e aos conceitos abstratos usados na produção.

A organização tem em sua tecnologia central, ou "*core technology"*, a principal tecnologia para a produção de bens e serviços para prover ao ambiente, auxiliada por outros tipos de tecnologia, indiretamente ligadas ao processo produtivo ou à adaptação ao ambiente.

As características tecnológicas nas organizações mudam ao longo do tempo, como se observa no período industrial, caracterizado pela produção em massa, e no período pós-industrial, onde a tecnologia traz maior flexibilidade à produção, como nos sistemas *just-in-time*. Estudos organizacionais sobre tecnologia conceberam tipologias para melhor compreender a variedade tecnológica e maneiras de organizá-las, como a tipologia de Charles Perrow.

Perrow (1967, 1986; *apud* Hatch,1997) reconheceu a diversidade tecnológica nas organizações, apresentando uma abordagem em duas dimensões: a capacidade analítica da tarefa e a variabilidade da tarefa. Por variabilidade da tarefa, Perrow considerou como o número de exceções encontradas em relação a procedimentos padrões em uma dada aplicação de tecnologia. Por capacidade analítica da tarefa, ele considerou a existência de métodos analíticos conhecidos para tratar as exceções encontradas. A Figura 5 apresenta a tipologia de Perrow.

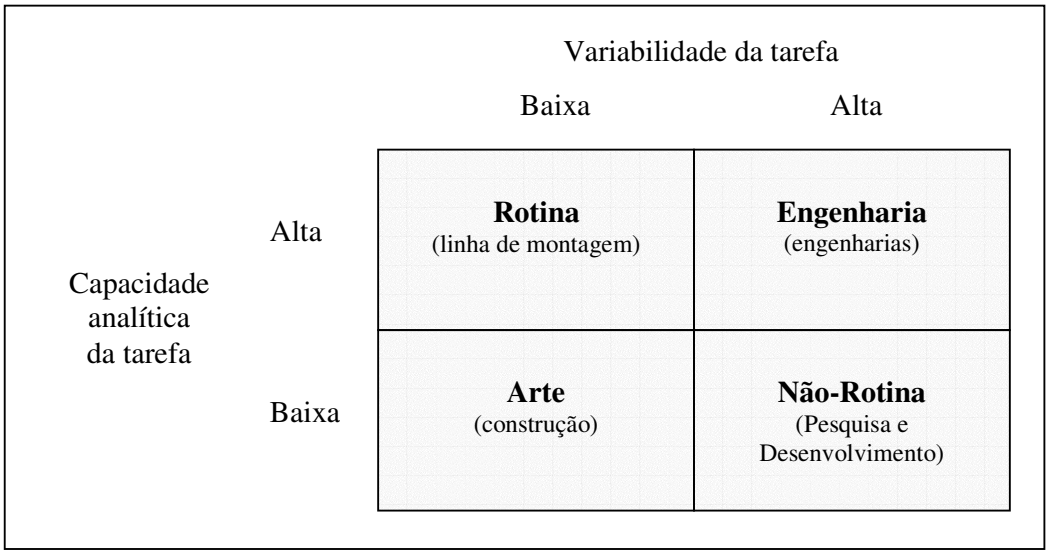


Figura 5 – Tipologia de Tecnologia para Perrow (Adaptado de Perrow, 1967, segundo Hatch, 1997, p. 141).

Weick (1990 *apud* Roberts e Grabowski, 1996; Hatch, 1997) afirma que os avanços na micro-eletrônica desafiam as tipologias da moderna teoria organizacional. Para ele, as novas tecnologias vão além das fronteiras conceituais daquelas proposições, sendo distinguidas por constituírem-se de eventos estocásticos, contínuos e abstratos.

Estocásticos no sentido de que as novas tecnologias tendem a formar uma densa interação de componentes, muitas vezes produzindo resultados não esperados, em caminhos aleatórios de execução. Os eventos contínuos das novas tecnologias caracterizam-nas pelo grau de automação, onde a atenção migra da eficiência para a confiabilidade. Por último, sua característica abstrata deve-se à crescente complexidade e a assimilação pelas máquinas do trabalho humano, em que o processo produtivo é realizado com base nos modelos cognitivos para sua compreensão.

Roberts e Grabowski (1996) dizem que uma das dificuldades nos estudos sobre tecnologia diz respeito a sua natureza sempre mutante. Muitas vezes as tecnologias atuais, como a tecnologia da informação, restringem e derrubam velhos modelos tecnológicos.

2.2.2 O Paradigma da Tecnologia da Informação

Dosi (1988, *apud* Cimoli e Giusta, 2003 p.51) define paradigma tecnológico como

> um padrão de solução para determinados problemas tecno-econômicos, baseado em princípios altamente selecionados derivados das ciências naturais, juntamente com regras específicas destinadas a adquirir novo conhecimento e protegê-lo, sempre que possível, da rápida difusão entre competidores.

Christopher Freeman, citado em Dosi *et al.* (1988, *apud* Castells, 1999 p.107), acrescenta que a estrutura de custos relacionada aos insumos para a produção é importante nas descobertas de inovações técnicas, organizacionais e administrativas de um paradigma econômico e tecnológico: “Em cada novo paradigma, um insumo específico ou conjunto de insumos pode ser descrito como o ‘fator-chave’ desse paradigma caracterizado pela queda dos custos relativos e pela disponibilidade universal.” Para Freeman, a mudança contemporânea de paradigma, o da tecnologia da informação, baseia-se, principalmente, “em insumos baratos de informação derivados do avanço da tecnologia em microeletrônica e de telecomunicações.”

O Quadro 2 apresenta um resumo dos paradigmas tecno-econômicos históricos, onde se pode perceber o fenômeno das ondas largas de crescimento econômico (PEREZ, 2003), que surgem a cada 50 ou 60 anos aproximadamente, difundindo um novo conjunto de tecnologias genéricas, capaz de transformar as indústrias existentes e criar outras no centro de sistemas tecnológicos radicalmente novos. Essas revoluções tecnológicas são descritas por Schumpeter (1939) como furacões de destruição criadora, conseqüência, principalmente, das inovações radicais e também das inovações incrementais.

Quadro 2 – Características dos paradigmas tecno-econômicos

Fase	**1º Paradigma**	**2º Paradigma**	**3º Paradigma**	**4º Paradigma**	**5º Paradigma**
Início e término	1770/80 a 1830/40	1830/40 a 1880/90	1880/90 a 1920/30	1920/30 a 1970/80	1970/80 a ?
Descrição	Mecanização	Força a vapor e ferrovia	Energia elétrica, engenharia pesada	Produção em massa, "fordismo"	Tecnologias da informação
Fator-chave	Algodão e ferro fundido	Carvão e transporte	Aço	Petróleo e derivados	Microeletrônica, tecnologia digital
Setores alavancadores de crescimento	Têxteis e seus equipamentos, fundição e moldagem de ferro e energia hidráulica	Máquinas e navios a vapor, máquinas ferramentas e equipamentos ferroviários	Engenharia e equipamentos elétricos, engenharia e equipamentos pesados	Automóveis e caminhões, tratores e tanques, indústria aeroespacial, bens duráveis e petroquímicos	Equipamentos de informática e telecomunicações, robótica, serviços info intensivos e Softwares.
Infra-estrutura	Canais e estradas	Ferrovias e navegação mundial	Energia elétrica	Auto-estradas, aeroportos e caminhos aéreos	Redes e sistemas e *information highways*
Outros setores crescendo rapidamente	Máquinas a vapor e maquinaria	Aço, eletricidade, gás, corantes sintéticos, engenharia pesada	Indústria automobilística e aeroespacial, rádio e telecomunicaçõe s, metais e ligas leves, bens duráveis, petróleo e plásticos	Fármacos, energia nuclear, microeletrônica e telecomunicações	Biotecnologia, nanotecnologia e atividades especiais
Países líderes	Grã-Bretanha, França e Bélgica	Grã-Bretanha, França e Bélgica, Alemanha e EUA	Alemanha, EUA, Grã-Bretanha, França, Bélgica, Suíça e Holanda	EUA, Alemanha, outros países da CEE, Japão, Rússia, Suécia, Suíça	Japão, EUA, Alemanha, Suécia, outros países da CEE, Taiwan e Coréia l
Países em desenvolvimento	Alemanha e Holanda	Itália, Holanda, Suíça, Áustria – Hungria	Itália, Áustria – Hungria, Canadá, Suécia, Dinamarca, Japão e Rússia	Países do leste europeu, Brasil, México, Argentina, Coréia, China, Índia e Taiwan	Brasil, México, Argentina, China, Índia, Indonésia, Turquia, Venezuela, Egito

Fonte: Lastres e Ferraz (1999, p. 34).

Perez (2003) adota os conceitos schumpeterianos de inovação incremental e radical. As inovações incrementais são as melhorias sucessivas nos produtos e processos existentes, guiadas por uma lógica previsível estabelecida dentro de uma trajetória natural – como chamam Nelson e Winter (2002) – do paradigma tecnológico. Já a inovação radical ocorre pela introdução de um produto ou processo realmente novo, que servirá como ponto de partida a uma nova trajetória técnica. Na década de 1970, no Vale do Silício – Califórnia, um novo paradigma tecnológico, centrado nas tecnologias da informação e comunicação (TIC), foi constituído e concretizou um novo estilo de produção, comunicação, gerenciamento e vida. Após a inovação radical do microprocessador, sucederam-se outras inovações incrementais, como a microcomputador, os avanços nas telecomunicações, a criação de redes de computadores. Castells (1999, p.98) afirma que o surgimento deste paradigma "não se originou de qualquer necessidade preestabelecida. Foi mais o resultado de indução tecnológica que de determinação social."

Assim, observa-se o caráter "*science push*" ou "*capabilities push*" da inovação tecnológica, no qual as atividades de P&D dão origem a desenvolvimentos tecnológicos, que por sua vez levam à produção industrial e comercialização das inovações (NELSON e WINTER, 2002). Por outro lado, a sua adoção nas organizações, do nível operacional ao estratégico, levou ao desenvolvimento de uma série de inovações incrementais, como softwares e hardwares periféricos, que indicam a característica "*demand pull*" das inovações, isto é, a percepção de uma necessidade ou demanda do mercado precede a inovação (NELSON e WINTER, 2002).

Conforme Roberts e Grabowski (1996), à medida que o poder de computação e as instalações de comunicação vêm melhorando, as empresas terão que moldar sua estratégia e estrutura para se ajustar a uma nova TI. A tecnologia da informação, que compreende as tecnologias mecânicas, humanas e de conhecimento, contribui para o desenvolvimento de eventos abstratos, contínuos e estocásticos em organizações.

2.2.3 O Componente de Tecnologia da Informação no Risco Operacional

Para Guldentops (2004), dentre os componentes do Basiléia II, a tecnologia da informação (TI) é mais relevante nas especificações qualitativas, que são gerenciamento de

riscos, controle e práticas de governança. Neste caso, a dimensão de TI é percebida no grande risco de descontinuidade de serviço em um ambiente mundialmente conectado, 24 horas, 7 dias por semana. A entrega de serviço no mundo financeiro é inteiramente dependente da tecnologia da informação e requer a confiabilidade de sistemas e integridade de informação.

No documento sobre as boas práticas para gestão do risco operacional (BIS, 2003), o Comitê da Basiléia observa que os eventos de desregulamentação e globalização dos serviços financeiros, aliados à crescente sofisticação da tecnologia, estão tornando as atividades dos bancos – e conseqüentemente seu perfil de risco – muito mais diversos e complexos.

Dentre os seis exemplos de riscos apresentados naquele documento, quatro são relacionados ao uso da TI: (i) o aumento da automatização tem potencial para transformar os riscos de erros do processamento manual em riscos de falhas de sistemas; (ii) o crescimento do comércio eletrônico introduz riscos potenciais ainda não completamente entendidos; (iii) integração de sistemas em virtude de aquisições, fusões e incorporações; e (iv) bancos atuando como provedores de serviços de larga-escala criam a necessidade de manutenção contínua de controles internos e sistemas de *backup*.

Guldentops (2004) relaciona princípios de boas práticas para gestão do risco operacional a aspectos de tecnologia da informação, conforme o Quadro 3.

Quadro 3 – Visão da Tecnologia da Informação nos Princípios do Basiléia II

Princípios de Boas Práticas	**Aspectos de Tecnologia da Informação (TI)**
1º Princípio: Conselho de Administração • Consciência do risco operacional (RO) • Estabelecimento de estrutura para gestão do RO • Revisão periódica	• Alinhamento estratégico negócio – TI • Entrega de valor de TI • Gestão de risco de TI • Medida de desempenho de TI
2º Princípio: Conselho de Administração • Assegurar auditoria interna eficaz • Auditoria interna independente, bem treinada e competente	• Crescimento da participação de TI nos programas de auditoria interna • Necessidade de demonstrar governança de TI • Necessidade de estrutura de controle para TI
3º Princípio: Gerência Sênior • Implementação da estrutura para RO • Desenvolvimento de políticas, processos e procedimentos	• Metodologias para compatibilizar riscos de TI, controles e questões técnicas

4º Princípio: Identificação e Avaliação • Produtos, atividades, processos e sistemas • Controle sobre as mudanças para adequação aos procedimentos de avaliação	• O negócio bancário é altamente dependente de sistemas de TI • TI está presente em quase todos os produtos, atividades e processos • TI é um dos maiores fatores de risco operacional
5º Princípio: Monitoração e Informação • Monitoração do perfil de RO • Informação proativa para o comitê de administração e gerências seniores	• TI é fundamental em sistemas de monitoramento e informação
6º Princípio: Política de Controle • Política, processos e procedimentos para controlar ou mitigar RO	• Como TI é essencial para o negócio, será parte significante da política de controle e risco do banco
7º Princípio: Planos de Contingência • Minimizar perda durante falhas operacionais com planos de contingência e continuidade	• O desenvolvimento de plano de recuperação de desastres (*disaster recovery plan)* envolve o planejamento de TI
8º e 9º Princípios: Supervisão Bancária • Avaliação de desenvolvimentos para gestão de riscos	• Estruturas para gestão de riscos operacionais envolvem a gestão de riscos de TI

Fonte: Adaptado de Guldentops (2004, p. 2)

Roessing (2005) também ressalta a importância da TI no contexto do Basiléia II. Ele observa duas dimensões associadas ao papel da TI. A primeira como uma ferramenta para implementação de estruturas para gerenciamento de riscos, e a segunda tendo o papel da TI como risco operacional em si mesma, nos sistemas operacionais que suportam o processamento bancário. Para Roessing (2005, p.2),

> A tecnologia da informação é um risco sistêmico para as operações bancárias. Por um lado, serve como uma ferramenta para gerenciar e reduzir risco operacional. Por outro lado, infra-estruturas complexas e aplicações [sistemas] criam significantes riscos que podem ir além das fronteiras de uma organização.

Em razão da complexidade inerente à maioria dos ambientes de tecnologia da informação de bancos, a relação causal entre os impactos na infra-estrutura e as perdas de negócio resultantes é de difícil diagnóstico. Muitas vezes, somente quando as falhas aparecem nos processos centrais de negócio é que as perdas se tornam aparentes. Conseqüentemente, o número de fatores de risco tecnológico a ser considerado para prevenir riscos de TI é vasto, e a prevenção específica de falhas de TI é proibitiva financeiramente (ROESSING, 2005).

Neste contexto, estruturas padrões de controle e governança têm sido desenvolvidas para satisfazer requisitos de confiabilidade e sustentabilidade da tecnologia da informação (ROESSING, 2005), como as citadas no item 2.1.5 deste trabalho (p. 30).

Em especial, a estrutura COBIT (*Control Objectives for Information and related Technology)* para governança de TI pode ser utilizada e será detalhada no item a seguir.

2.3 Governança Corporativa e de Tecnologia da Informação

Este item, o penúltimo do referencial teórico-empírico, traz a conceituação de governança corporativa, gestão de riscos e controle interno, os quais são incorporados também pela governança de tecnologia da informação. A partir do Basiléia II, busca-se relacionar eventos de riscos, princípios para gestão do risco operacional e cenário de uso de TI a objetivos de controle de TI. Em seguida, o *framework* COBIT é detalhado e faz-se a escolha de alguns de seus processos para compor o modelo conceitual da pesquisa empírica.

2.3.1 Governança Corporativa, Gestão de Riscos e Controle Interno

Originalmente, o conceito de governança corporativa abrangia apenas os conflitos entre proprietários e administradores em empresas de propriedade pulverizada, em que posse e controle são exercidos por diferentes agentes, com orientações diversas (PFEFFER, 1972; DONALDSON e DAVIS, 1994 *apud* MEIRELLES *et al.*, 2005). Desta forma, a boa governança atenderia à minimização de custos de agência e de riscos dos acionistas.

A acepção do termo governança é analisada por Turnbull (1997), que evidencia o seu crescente uso contemporâneo em disciplinas como economia organizacional, teoria organizacional, teoria da informação, direito, contabilidade, administração, sociologia e política. Cada uma delas pode ter uma visão diferente para o termo governança corporativa, por motivos de objeto de análise, como mostra o Quadro 4. Muitas vezes, ocorre ambigüidade no significado de termos-chave como controle, regulamentação, gestão, governo e governança.

Quadro 4 – Objetos de análise e variáveis relacionadas a governança corporativa

Autores	Objeto de análise	Variável
Simon, 1962	Informação	Gestão da complexidade
Turnbull 1975, 1993	Responsabilidade de gestores	Gestão de conflitos
Jensen & Meckling, 1976	Custo de agência	Estrutura financeira
Williamson, 1985	Custo de transação	Organização industrial
Hollingsworth & Lindberg, 1985	Quatro modos de governança	Organização social
Monks & Minow 1991, 1995, 1996	Transparência do conselho de administração	Investimento em relações
Demb & Neubauer, 1992	*Stakeholders*	Responsabilidade da firma
Cadbury, 1992	Aspectos financeiros	Conformidade do conselho de administração
Porter, 1992	Natureza da propriedade	Competitividade da firma
Hilmer, 1993	Reunião do conselho administrativo	Desempenho da firma
Jensem, 1993	Empresas de capital aberto	Falha no sistema de controle
Boschm 1995; AIMA 1995	Deveres dos gestores	Código de conduta
Sternberg, 1996	Apropriação por *stakeholders*	Valor para o acionista
Hawley & Williams, 1996	Capitalismo fiduciário	Desempenho corporativo
Shleifer & Vishny, 1996	Riscos morais	Retorno de investimento
Persson *et al*., 1996	Separação de poderes	Bem-estar dos *stakeholders*

Fonte: Turnbull (1997, p. 185)

Para Turnbull (1997, p.181), governança corporativa "descreve todas as influências que afetam os processos institucionais, incluindo aqueles para escolha de controladores e/ou reguladores, envolvidos na organização da produção e venda de bens e serviços."

Demb e Neubauer (1992, *apud* Turnbull, 1997, p.184) afirmam que a "governança corporativa é o processo pelo qual as organizações se tornam responsáveis pelos direitos e expectativas dos *stakeholders*."

Tricker (1994, *apud* Turnbull, 1997, p.184) declara que "governança corporativa trata dos assuntos envolvendo o conselho administrativo, como as interações com a alta gerência e relacionamentos com os proprietários e outros interessados nos negócios da empresa, incluindo credores, financiadores de dívida, analistas, auditores e reguladores corporativos."

Já Donaldson (1990, *apud* Turnbull, 1997, p.184) define governança corporativa como "a estrutura por meio da qual gerentes no vértice organizacional são controlados pelo conselho administrativo, suas estruturas associadas, incentivos executivos, e outros esquemas de monitoramento e ligação."

Hawley e Williams (1996 *apud* Turnbull, 1997) realizaram revisão da literatura sobre governança corporativa, base para publicações da Organização para Cooperação e Desenvolvimento Econômico (OCDE) nesta área de conhecimento, como "*OECD Principles of Corporate Governance*", publicado em 1999 e revisado em 2004, com foco geral nas empresas de capital aberto (OCDE, 2004). A governança corporativa foi descrita como um sistema por meio do qual as empresas são dirigidas e controladas.

Alinhado aos princípios de governança corporativa da OCDE, o Banco de Compensações Internacionais (BIS) elaborou em 1999, com revisão em 2006, o documento "*Enhancing Corporate Governance for Banking Organizations"* (BIS, 2006), com o objetivo de assistir as organizações bancárias na melhoria de suas estruturas de governança corporativa e também auxiliar os órgãos supervisores na avaliação da qualidade de tais estruturas, uma vez que elas são essenciais para a manutenção da confiança pública no sistema financeiro.

No âmbito bancário, a governança corporativa se relaciona à maneira pela qual os negócios são conduzidos pelo conselho administrativo e gerentes seniores, envolvendo: a definição de objetivos; as operações diárias; a transparência na divulgação de informações; a proteção dos direitos dos depositários; o alinhamento das atividades e comportamento às expectativas de operação do banco, de maneira segura e em conformidade com as leis e regulamentações (BIS, 2006).

Para a OCDE (2004) e o BIS (2006), o conceito de governança corporativa expressa um conjunto de relações entre os gestores, o conselho, os acionistas e outros *stakeholders* da empresa, em que se desenvolve uma estrutura para o estabelecimento de objetivos

estratégicos, seus recursos e formas de monitoramento, e ainda proporciona adequados incentivos aos gestores para o alcance dos interesses da empresa e de seus acionistas.

Meirelles *et al.* (2005) vêem, à luz dos entendimentos correntes e evidências empíricas, que a governança corporativa deve ser sustentada por alguns pilares, como a prestação de contas ou responsabilização (*accountability)*, transparência (*disclosure*), código de ética e gestão e controle de riscos.

A Figura 6 apresenta alguns aspectos dos princípios para uma boa governança, indicados pelo Comitê da Basiléia para Supervisão Bancária (BIS, 2006). Percebe-se nesta publicação a importância da gestão de riscos e do sistema de controles internos para a eficácia de sua implantação. Esses relacionamentos – governança corporativa, gestão de riscos e controles internos – também são demonstrados por Holm e Laursen (2007).

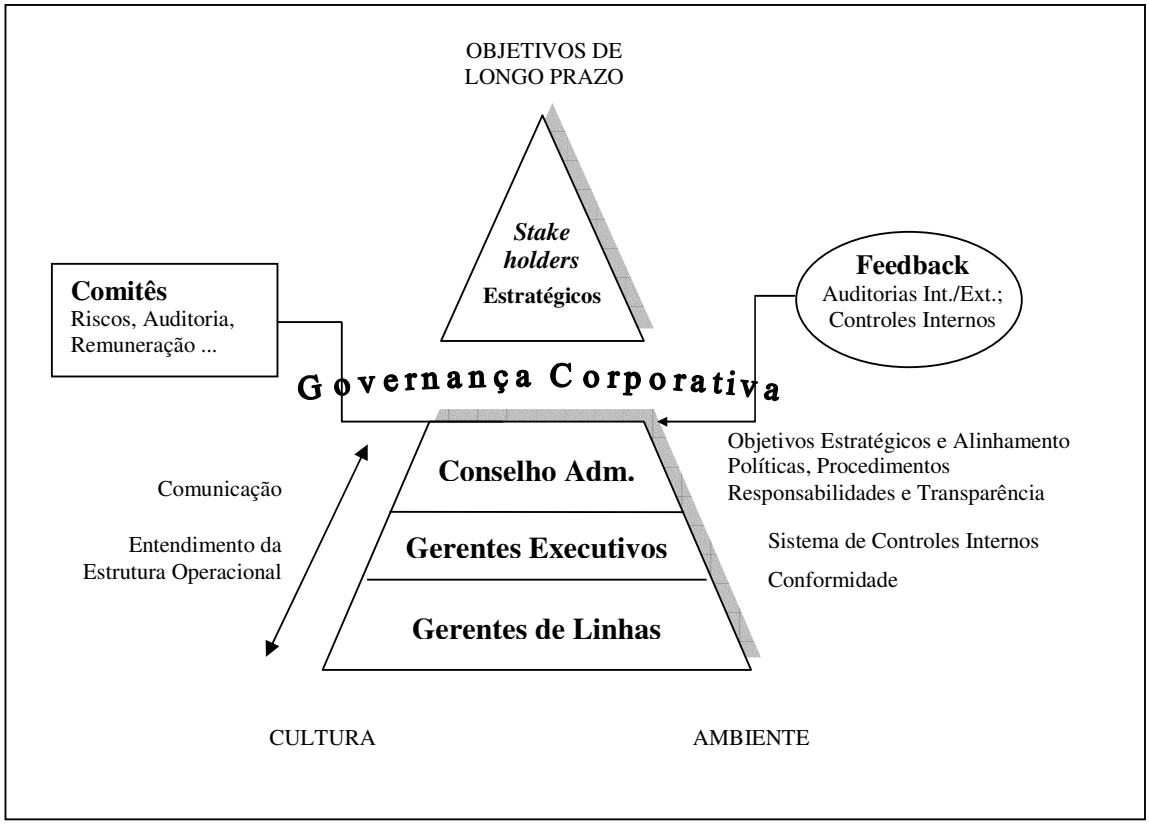


Figura 6 – Princípios de Governança Corporativa

Fonte: o autor, a partir de BIS, 2006

Por sua vez, a gestão corporativa de riscos é conceituada em COSO (2004, p. 2) como

> um processo liderado pelo conselho administrativo da empresa, gestores e outros funcionários, aplicado na definição estratégica e projetado em todos os níveis para identificar eventos potenciais que possam afetar a entidade, gerenciar riscos dentro do apetite a riscos e prover segurança adequada para o alcance dos objetivos da empresa.

Tannenbaum (1975) analisa as nuanças no conceito de controle, que é empregado muitas vezes como sinônimo de poder, autoridade e influência. Ele usa o conceito de controle como um "processo, no qual uma pessoa, grupo de pessoas ou organizações de pessoas determinam, i. é, intencionalmente afetam, o comportamento de uma outra pessoa, grupo ou organização" (p. 18). Tannenbaum (1975) apresenta o processo de controle como um ciclo, em que a intenção de uma pessoa A é seguida por uma tentativa de influência dirigida a outra pessoa B, que age executando a intenção de A.

Neste trabalho, o conceito de controle aproxima-se de sua utilização inicial nas empresas de negócios, como afirma Tannenbaum (1975, p. 18): "deriva do significado francês, como sinônimo de fiscalizar". Adota-se aqui esse sentido, mas sem o intuito de punição, antes de ajuste ou correção das ações para o alcance de objetivos, mais próximo de um monitoramento.

A importância do controle para a gestão de riscos também é abordada em NIST (2002). Os controles implementados ou planejados são "medidas para redução de riscos" (p. 2), ou seja, ações para minimizar ou anular a probabilidade de uma ameaça valer-se de uma vulnerabilidade do sistema, conforme a Figura 7.

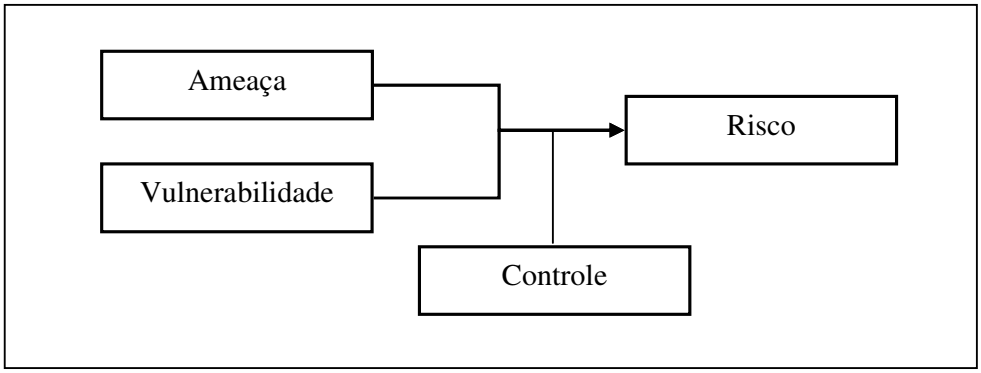


Figura 7 –Controles como forma de redução de riscos (O autor, a partir de NIST, 2002)

Ameaça é o "potencial para uma determinada fonte de ameaças exercer uma vulnerabilidade em particular" (NIST, 2002, p.12). Vulnerabilidade é "uma fraqueza no projeto, implementação ou procedimentos de segurança de sistemas, ou em controles internos, que pode ser explorada (acidentalmente disparada ou explorada intencionalmente) e resulta em uma quebra de segurança ou violação da política de segurança de sistemas" (NIST, 2002, p. 15). Os métodos de controles podem ser técnicos (incorporados em hardware ou software) ou não técnicos (políticas, procedimentos), nas categorias de prevenção ou de detecção.

Controle interno, para COSO (1994) e BIS (1998), é um processo contínuo conduzido em todos os níveis da organização, especificando políticas e procedimentos com objetivos:

(i) operacional - eficácia e eficiência;

(ii) de informações - completas e confiáveis; e

(iii) de conformidade – a leis e regulamentações.

Bergamini Jr (2005) salienta a divisão entre controles internos contábeis e administrativos, estes referentes a procedimentos relacionados à eficiência operacional e aqueles à fidedignidade dos registros contábeis.

Ainda para COSO (1994) e BIS (1998), cinco elementos constituem um adequado sistema de controles internos: (i) ambiente de controle – base de todos os elementos de controle interno, que inclui os valores e competências essenciais à empresa, influenciando a cultura e estrutura organizacionais; (ii) avaliação de riscos – a identificação e a análise de riscos que vão de encontro aos objetivos; (iii) atividades de controle – tarefas de controle específicas para controle dos riscos identificados; (iv) informação e comunicação – via dupla de informação entre gestores e funcionários; e (v) atividades de monitoramento – avaliação e apreciação dos controles internos.

Para cobrir riscos de crédito, de mercado, de liquidez e operacional, a avaliação de riscos deve identificar fatores internos e externos que possam afetar o cumprimento de objetivos operacionais, de informação e de conformidade da organização. Para a identificação desses fatores nas atividades de tecnologia da informação, o constructo governança corporativa é então incorporado e estendido pela governança de TI, que tem por finalidade o atendimento aos *stakeholders* internos da organização.

Para Lainhart IV (2000, p. 34), "a governança de TI funciona de maneira similar à governança corporativa, embora em um ambiente mais focado". A Figura 8 exprime a interdependência entre governança e atividades de tecnologia da informação.

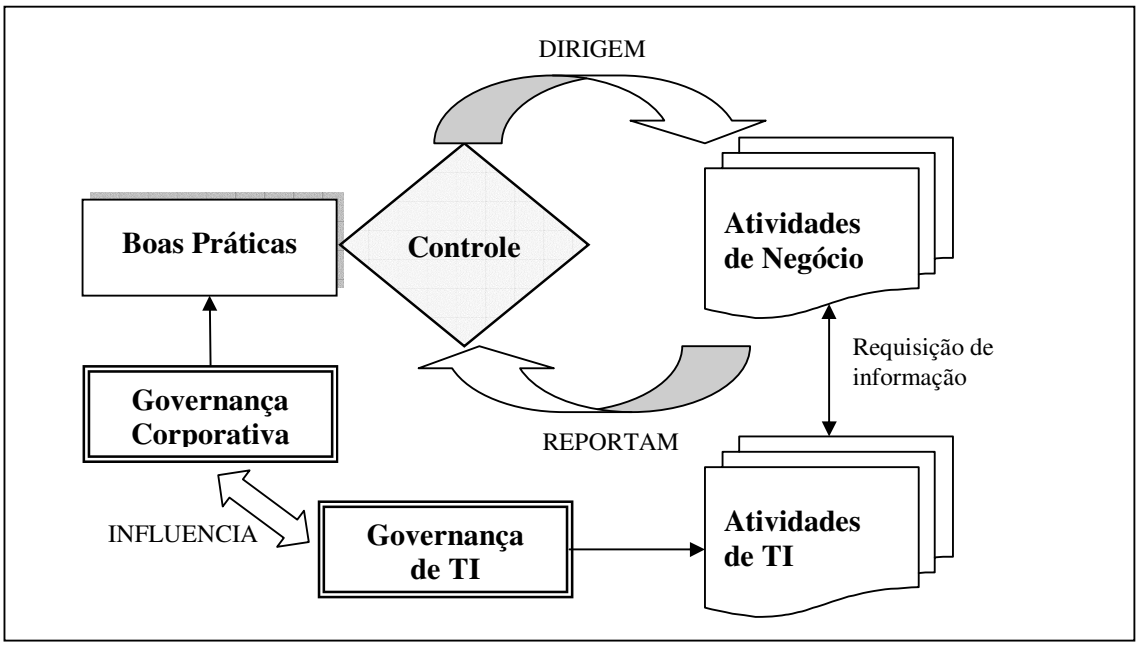


Figura 8 –Governança Corporativa e Governança de TI (Adaptado de Lainhart IV, 2000)

2.3.2 Governança de Tecnologia da Informação

As tecnologias de informação e comunicação (TIC) fornecem suporte a múltiplos processos de negócio no setor financeiro, muitas vezes criando redes interorganizacionais, com aplicações fortemente integradas. Em uma perspectiva de risco operacional, as inovações tecnológicas presentes nessas redes e a sua importância para o funcionamento de um sistema bancário criam vulnerabilidades e riscos complexos, muitas vezes sistêmicos. "O mundo da tecnologia da informação tem se tornado de maior risco em conseqüência de otimizações e remoção de *buffers* entre os processos." ROESSING (2005, p. 4)

Roessing (2005) observa a necessidade de um alinhamento entre a gestão de riscos de TI e os principais processos de negócio nas estruturas para gestão do risco corporativo. Os aspectos preventivos para a mitigação de riscos de TI envolvem políticas preventivas, instruções detalhadas de controle e elaboração de processos e ferramentas de monitoração.

Para o ITGI (2007), uma governança eficaz de tecnologia da informação gerencia apropriadamente riscos e oportunidades relacionadas ao uso de TI, bem como promove o suporte de TI aos objetivos do negócio e otimiza o investimento em TI.

Weill e Ross (2006) entendem que a governança de TI está relacionada à estrutura de responsabilidades para estimular comportamentos desejáveis na utilização da TI e ainda à especificação dos direitos decisórios. Nessa linha, em ITGI (2005, p.5) encontra-se que "governança de TI é uma responsabilidade dos executivos e do conselho administrativo, e consiste em processos, estruturas e liderança organizacionais que garantam que a tecnologia da informação corporativa sustente e estenda as estratégias e objetivos da organização".

Com o propósito de gerenciar riscos e realizar os objetivos da empresa, as atividades de TI também são conduzidas de acordo com boas práticas, caracterizadas nos processos de planejamento e organização, aquisição e implementação, entrega e suporte, e monitoramento, conforme a Figura 9. A governança de TI agrega segurança, confiabilidade e conformidade para atingir os objetivos da governança corporativa (LAINHART IV, 2000).

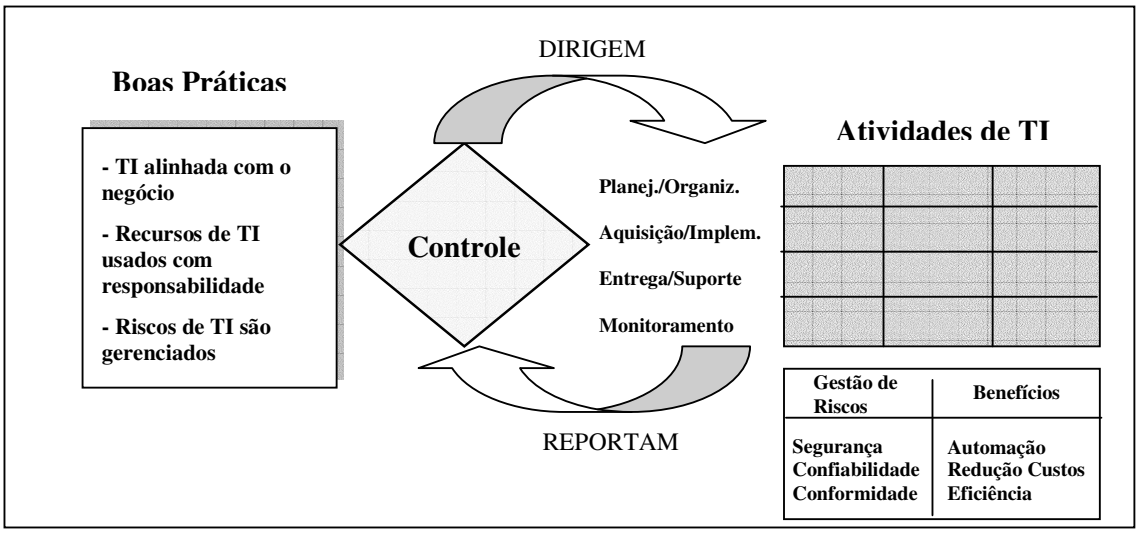


Figura 9 –Governança de TI (Adaptado de Lainhart IV, 2000, p. 36)

Albertin e Albertin (2005) relacionam a governança de TI à autoridade e responsabilidade pelas decisões referentes ao uso de TI e sua administração. Para o uso eficaz de TI, os processos de planejamento, organização, direção e controle devem ser considerados, desde seu alinhamento estratégico até a mensuração dos seus impactos de desempenho. Os esforços de executivos de negócio e de executivos de TI devem convergir para o aproveitamento de oportunidades, sendo a participação desses últimos particularmente importante por pertencerem a uma área que permeia todas as outras e está em contato direto com as inovações tecnológicas.

Pinochet *et al.* (2005) acrescentam que a governança de TI tem levado a um conjunto de práticas de gestão com foco em direção e controle, com base na interação entre os atores que participam do processo decisório. Alguns aspectos importantes são identificados: (i) acesso interno e externo à informação; (ii) interação entre os atores; (iii) monitoramento; (iv) transparência, equidade e ética; e (v) responsabilidade por decisões.

Em resumo, o ITGI (2005) salienta os principais objetivos da governança da tecnologia da informação: (i) assegurar o alinhamento estratégico entre TI e negócio; (ii) buscar com que a TI suporte o negócio e maximize a entrega de valores; (iii) garantir o uso adequado dos recursos de TI; e (iv) gerenciar apropriadamente os riscos de TI.

Para isso, as suas atividades têm foco em cinco áreas de atuação, descritas na Figura 10. Alinhamento estratégico e entrega de valor são resultados, enquanto que medida de desempenho, gestão de recursos e gestão de riscos são direcionadores da governança.

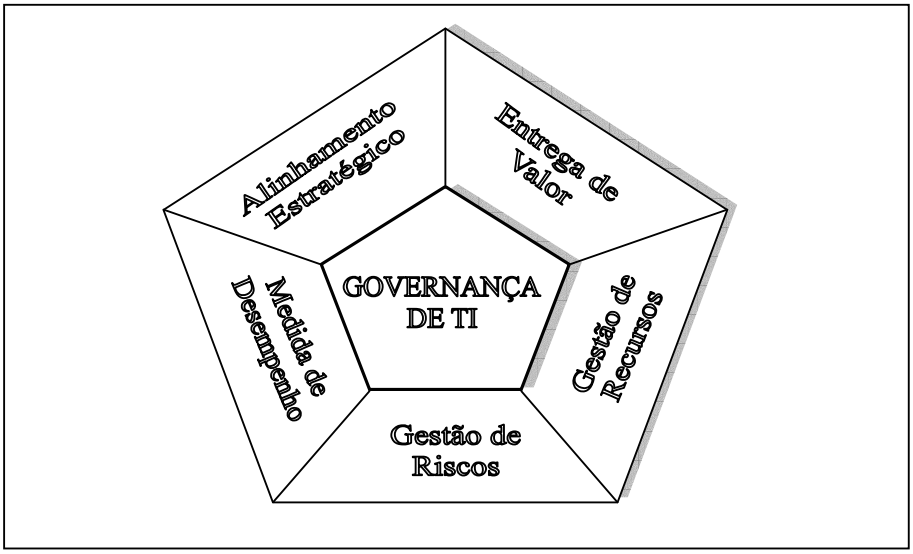


Figura 10 –Foco de Atuação da Governança de TI (ITGI, 2005)

Alcançando essas cinco áreas de atuação, os processos de controle são partes constituintes da governança de TI. A excelência ou maturidade na condução desses processos relaciona-se ao controle e à mitigação do risco operacional em seu componente de tecnologia da informação.

2.3.3 Análise de Cenários e Objetivos de Controle para TI

Para a utilização dos métodos padronizado e avançado especificados no Basiléia II (BIS, 2004), mostrados na Figura 2 (p. 29), as instituições financeiras devem realizar o registro e a manutenção de informações acerca de riscos operacionais relacionados aos tipos de eventos enumerados naquele acordo, os quais possuem, em sua maioria, fonte de risco relacionada à tecnologia da informação. Guldentops (2004) aponta os aspectos de TI que podem estar vinculados a cada um dos eventos de perda, conforme o Quadro 5.

Quadro 5 – Tipos de Eventos de Risco no Basiléia II e sua Relação aos Aspectos de TI

Tipo de Evento	Aspectos de TI
Fraude Interna	Manipulação deliberada de software e hardware; Uso não autorizado de funções; Mudança deliberada de dados; Uso de cópia não licenciada de software; Sistema de privilégios deficiente
Fraude Externa	Alteração de sistemas e dados por *hacker*; Interceptação do sistema de comunicação; Vírus; Senhas comprometidas;
Práticas de Emprego e Segurança do Ambiente	Mau uso de recursos de TI; Falha na responsabilidade de segurança de TI
Clientes, Produtos e Práticas de Negócio	Divulgação de informação sigilosa para fora da organização; Gestão de serviços terceirizados
Danos a Ativos Físicos	Danos deliberados ou acidentais a infra-estrutura de TI
Rompimento de Negócio e Falha de Sistema	Defeito em hardware ou software; Falha na rede; Sabotagem; Perda de funcionários-chave; Destruição de banco de dados; Falha de backup; Erro de configuração
Execução, Entrega e Gestão de Processos	Transações incompletas; Erros de programação ou teste; Erro de operação; Procedimentos manuais falhos

Fonte: Adaptado de Guldentops (2004, p. 3)

Da mesma forma, encontram-se nas "Boas Práticas para o Gerenciamento e Supervisão do Risco Operacional" (BIS, 2003) alguns aspectos relevantes relacionados a TI, conforme o Quadro 6.

Quadro 6 – Relevância de TI nos princípios para gestão do risco operacional

Princípio da Basiléia	**Relevância para TI**
1. Consciência do Risco Operacional pelo Conselho Administrativo	Gestão de risco de TI
2. Estrutura de gestão do Risco Operacional sujeita à auditoria interna	Auditoria interna de TI
3. Políticas, procedimentos e processos para gestão do Risco Operacional	Gestão de risco de TI
4. Identificação e avaliação do Risco Operacional	Gestão de risco de TI
5. Monitoramento do perfil de Risco Operacional	Gestão de risco de TI
6. Políticas, procedimentos e processos para controle e mitigação do Risco Operacional	Gestão de risco de TI
7. Planos de contingência e continuidade de negócio	Garantia de continuidade de serviço
8. Estrutura para identificar, avaliar, monitorar e controlar/mitigar Riscos Operacionais	Gestão de risco de TI
9. Avaliação independente de políticas, procedimentos e práticas relacionadas a Riscos Operacionais	Auditoria interna de TI
10. Divulgação pública	Intensificação de TI para a gestão

Fonte: Adaptado de ITGI (2007, p. 42)

A utilização dos Métodos Avançados para a alocação de capital para risco operacional prevê a utilização de análise de cenários e opiniões de especialistas, além de dados externos para a avaliação de exposições a eventos de alta severidade. A análise de cenários favorece a consolidação de experiências de especialistas em TI, segurança da informação, gerentes de negócio e de riscos, assim como as visões da auditoria interna (ITGI, 2007). Bergamini Jr (2005) observa a mudança do foco nos trabalhos de auditoria interna para o controle interno sob a ótica de riscos. Uma exemplificação de análise de cenário é mostrada no Quadro 7.

Quadro 7 – Cenários de TI e Objetivos de Controle

Cenário	Descrição	Objetivo de Controle
Usuário autorizado realiza atividades não autorizadas	Usuários possuem acesso a funções mas fazem uso indevido, como manipulação de sistemas, alteração de dados ou manipulação de dados de entrada	Garantir a segurança de sistemas
Rompimento de serviço	Ocorre falha em hardware ou software, serviço crítico ou ambiente de sistemas; ausência de serviço; erro de planejamento de capacidade	Garantir a continuidade de serviço
Processo de transação incompleto	Ocorrência de resultados indesejados em função de falhas no processo de transação de dados	Garantir a integridade e validade de dados
Mau uso de informações sigilosas	A autorização de acesso pode gerar mau uso de informações privilegiadas	Garantir a segurança de sistemas
Falha de projeto	Projetos não são entregues de acordo com cronograma, orçamento e qualidade	Assegurar a gerência de projetos

Fonte: Adaptado de ITGI (2007, p.37 e 44)

Com base nas publicações do BIS – Acordo da Basiléia II (BIS, 2004) e "Boas Práticas para o Gerenciamento e Supervisão do Risco Operacional" (BIS, 2003) – e ainda na estrutura COSO para gestão corporativa de riscos – "*Enterprise Risk Management – Integrated Framework"* COSO (2004) – o ITGI (2007) elaborou alguns princípios para a aplicação de objetivos de controle de TI nos aspectos de risco operacional, conforme o Quadro 8.

Quadro 8 – Princípios para aplicação de objetivos de controle

Princípio	Nome	Descrição
01	Consciência do Risco Operacional	TI forma uma parte crítica da gestão do risco operacional. Técnicos, auditores internos e profissionais de finanças devem ter essa consciência.
02	Auditoria Interna	A função de auditoria interna de TI deve ser eficaz e ampla, valendo-se de capacitação profissional, recursos e orçamento para tal.
03	Política, Procedimentos e Processos de Gestão	A gestão da informação e tecnologia deve ser dirigida por um conjunto de políticas, procedimentos e processos para a gestão de riscos.
04	Avaliação de Risco	Avaliações de risco específicas devem ser conduzidas, usando abordagem compatível com a estrutura corporativa de governança, gestão de riscos e conformidade.
05	Monitoramento de Riscos e Perdas	Perdas relacionadas à gestão de informação e tecnologia devem ser medidas e documentadas.
06	Políticas, Procedimentos e Processos para Controle e Mitigação	A gestão da informação e tecnologia deve ser dirigida por um conjunto de políticas, procedimentos e processos para o controle e mitigação de riscos, em linha com a estrutura corporativa de governança, gestão de riscos e conformidade.
07	Gestão da Continuidade de Negócio	A gestão da informação e tecnologia deve ser protegida por um processo de continuidade de negócio (*Business Continuity Plan*)
08	Estrutura para Controle e Mitigação de Risco	A gestão da informação e tecnologia deve ser parte integrante da estrutura corporativa de governança, gestão de riscos e conformidade.
09	Avaliação Independente	A gestão da informação e riscos relacionados a TI deve ser adequadamente documentada para suporte ao processo supervisão. A função de auditoria externa deve realizar revisões na gestão do risco operacional relacionado a TI.
10	Divulgação	Técnicos, auditores internos e profissionais de finanças devem identificar e comunicar riscos de TI aos *stakeholders*, como definido na estrutura corporativa de governança, gestão de riscos e conformidade.

Fonte: ITGI (2007, p. 23)

Alguns desses princípios fundamentam-se no alinhamento de processos de riscos de TI à estrutura corporativa para gestão de riscos. Para o ITGI (2007), a gestão corporativa de riscos abrange: o alinhamento da estratégia e apetite ao risco; responsabilidade nas decisões sobre respostas a riscos (evitação, redução, compartilhamento e aceitação); redução de perdas

e surpresas operacionais; identificação e gerenciamento de riscos múltiplos e inter-relacionados; reconhecimento de oportunidades; melhoria na alocação de capital.

Ainda para o ITGI (2007, p.32), na gestão de TI "as iniciativas e os programas para gerenciamento de risco devem ser integradas à abordagem mais ampla de governança, riscos e conformidade."

O princípio nº 9, Avaliação Independente, evidencia a importância da documentação de riscos relacionados a TI para possibilitar e dar suporte ao processo de supervisão. Nesse sentido, "as organizações devem adotar uma avaliação holística da capacitação e maturidade de sua estrutura para gerenciamento de riscos" (ITGI, 2007b, p. 32), onde capacitação e maturidade se referem, respectivamente, ao quão bem o processo funciona e à medida da intensidade do desenvolvimento da capacitação.

A revisão da literatura aponta para alguns modelos de governança de tecnologia da informação, como o ITIL (*IT Infrastructure Library)* e o COBIT (*Control Objectives for Information and Related Technology)* (LAINHART IV, 2000; ALBERTIN e MOURA, 2004; BRODBECK *et al.*, 2004; CAZASSA, 2005; OLIVEIRA *et al.*, 2005; ZORELLO, 2005; CAMPANÁRIO *et al.*, 2005; SOLMS, 2005; BORITZ, 2005; ROESSING, 2005; EEDE e WALLE, 2005; HARDY, 2006; BRODERICK, 2006; ITGI, 2007).

Hardy (2006) posiciona o COBIT como uma estrutura com liderança emergente para obtenção de eficácia na governança de TI. Cazassa (2005) evidencia a adoção desse modelo por grandes organizações, especialmente no setor financeiro.

2.3.4 Modelo COBIT para Governança de TI

O *framework* COBIT (*Control Objectives for Information and Related Technology)* (ITGI, 2007b) é resultado de esforços do Information Technology Governance Institute (ITGI), que desde 1998 vem atuando, com apoio de pesquisadores e profissionais distribuídos globalmente, para a consolidação de uma estrutura padrão aberta para governança de TI, a partir de padrões globais relacionados à tecnologia da informação, como os seguintes:

- Committee of Sponsoring Organizations of the Treadway Commission (COSO): *Internal Control – Integrated Framework* e *Enterprise Risk Management – Integrated Framework;*
- Office of Government Commerce: *IT Infrastructure Library* (ITIL);
- International Organisation for Standardisation: ISO/IEC 17799 – Práticas para gestão da segurança da informação;
- Project Management Institute (PMI): *Project Management Body of Knowledge* (PMBOK);
- Information Security Forum: *The Standard of Good Practice for Information Security*; e
- Software Engineering Institute (SEI): *Capability Maturity Model* (CMM).

Baseado na interação apresentada na Figura 11 e para responder a requisitos de desempenho e monitoramento, a estrutura COBIT fornece definições para *benchmarking* de capacitação em processos, expressos por modelos de maturidade derivados do *Capability Maturity Model* do SEI; métricas e objetivos para processos de TI para medida de resultados e desempenho, orientados pelos princípios do *Balance Scorecard* (BSC); e planos de atividades para controle desses processos, com base em objetivos de controles detalhados.

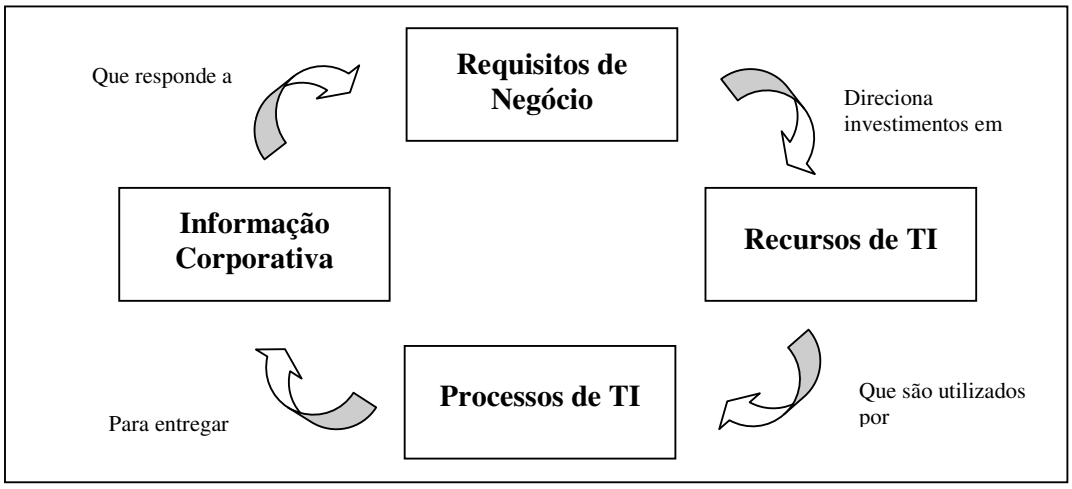


Figura 11 –Princípios Básicos do COBIT (ITGI, 2007b, p. 10)

Desta forma, a estrutura proposta busca suportar a governança de TI por meio do alinhamento aos requisitos de negócio, suporte ao negócio e maximização de benefícios, uso adequado dos recursos de TI e gerenciamento apropriado de riscos de TI. Ela propõe um modelo de referência para profissionais de tecnologia da informação e de negócio, com processos que normalmente são encontrados nas funções de TI na organização. As principais características do COBIT são o foco nos negócios, a orientação por processos, sua base em controles e o estímulo por medidas.

O modelo é composto por 34 processos de tecnologia da informação, distribuídos em 4 áreas de domínio, que são (1) Planejamento e Organização, (2) Aquisição e Implementação, (3) Entrega e Suporte e (4) Monitoramento e Avaliação. Essas áreas de domínio têm seu foco, respectivamente, na provisão de diretrizes de governança de TI, na provisão de soluções de serviços de TI, no oferecimento dos serviços aos usuários e no monitoramento dos processos para garantir o cumprimento dos objetivos necessários. O Quadro 9 apresenta todos os processos do modelo.

Quadro 9 – Processos de Governança de Tecnologia da Informação – Modelo COBIT versão 4.1

Domínio	**Nome dos Processos**
Planejamento e Organização	PO1 – Definição de plano estratégico de TI PO2 – Definição da arquitetura de informação PO3 – Determinação da direção tecnológica PO4 – Definição dos processos de TI, organização e relacionamentos PO5 – Gestão do investimento em TI PO6 – Comunicação dos objetivos de gestão e direcionamentos PO7 – Gestão de recursos humanos de TI PO8 – Gestão da qualidade PO9 – Avaliação e gestão de riscos de TI PO10 – Gestão de projetos
Aquisição e Implementação	AI1 – Identificação de soluções automatizadas AI2 – Aquisição e manutenção de softwares AI3 – Aquisição e manutenção de tecnologias de infra-estrutura AI4 – Habilitar operação e uso AI5 – Selecionar recursos de TI AI6 – Gestão de mudanças AI7 – Instalação e certificação de soluções e mudanças

Entrega e Suporte	DS1 – Definição e gestão de níveis de serviço DS2 – Gestão de serviços terceirizados DS3 – Gestão de desempenho e capacitação DS4 – Asseguração da continuidade de serviço DS5 – Asseguração da segurança de sistemas DS6 – Identificação e alocação de custos DS7 – Educação e treinamento de usuários DS8 – Gestão de serviços de apoio ao usuário e de incidentes DS9 – Gestão da configuração DS10 – Gestão de problemas DS11 – Gestão de dados DS12 – Gestão do ambiente físico DS13 – Gestão das operações
Monitoramento e Avaliação	ME1 – Monitoramento e avaliação do desempenho de TI ME2 – Monitoramento e avaliação de controles internos ME3 – Asseguração da conformidade com requisitos externos ME4 – Promoção de governança de TI

Fonte: ITGI (2007b, p. 26)

Gerke e Ridley (2006) realizaram um estudo nas organizações do setor público australiano e corroboraram os achados de pesquisas realizadas em outros países, como a de Guldentops *et al.* (2002), que avaliaram o potencial de utilização do modelo COBIT. Dentre os processos considerados como mais importantes por auditores e profissionais de TI, estão: Asseguração de segurança de sistemas (DS5); Asseguração da continuidade de serviço (DS4); Definição de plano estratégico de TI (PO1); Gestão de dados (DS11); Gestão de operações (DS13); Gestão de mudanças (AI6); Gestão de investimento em TI (PO5); Avaliação e gestão de riscos (PO9); e Gestão de projetos (PO10).

Na estrutura de processos do modelo COBIT, mostrada no Quadro 9, há ênfase nos aspectos de controle interno e promoção da governança de TI no domínio Monitoramento e Avaliação. Nesse modelo, controle é definido como "políticas, procedimentos, práticas e estruturas organizacionais projetadas para prover segurança de que os objetivos de negócio serão alcançados e eventos indesejados serão prevenidos ou detectados e corrigidos" ITGI (2007b, p. 13). A orientação para controle no modelo é a apresentada na Figura 12.

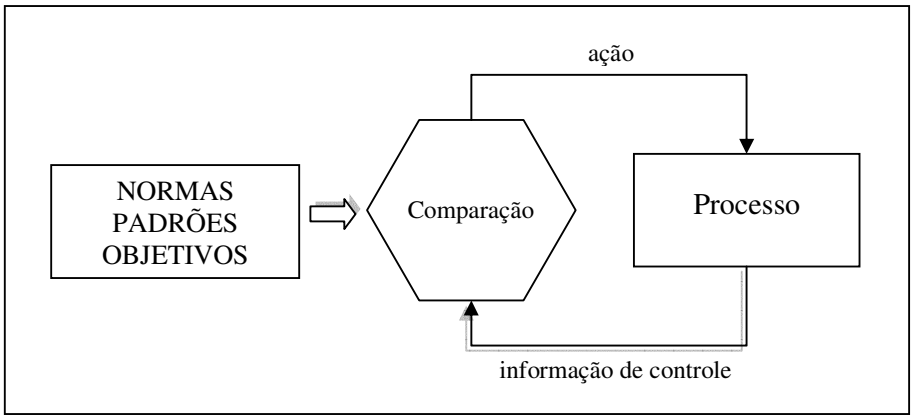


Figura 12 –Modelo de Controle (ITGI, 2007b, p. 14)

No modelo descrito na Figura 12 percebe-se a presença da aprendizagem de circuito simples (*single loop-learning)*, que consiste na tomada de ação em função dos valores, planos e regras organizacionais estabelecidos, sem, contudo, questioná-los. (ARGYRIS e SCHON, 1978 *apud* SMITH, 2001; SENGE, 1990 *apud* JIMÉNEZ-JIMÉNEZ e CEGARRA-NAVARRO, 2006).

Para auxiliar no diagnóstico da intensidade do funcionamento dos processos de TI, isto é, na sua capacitação e maturidade, um modelo de referência é definido para cada um dos processos que compõem a estrutura COBIT.

2.3.5 Gestão de Processos por Níveis de Maturidade

Conforme Gonçalves (2000), as organizações são grandes coleções de processos, os quais podem ser definidos como

> qualquer trabalho que seja recorrente, afete algum aspecto da capacitação da empresa (*organizational capability*), possa ser realizado de várias maneiras distintas com resultados diferentes em termos da contribuição que pode gerar com relação a custo, valor, serviço ou qualidade e envolva a coordenação de esforços para a sua realização (KEEN, 1997 *apud* Gonçalves, 2000, p. 8).

Partindo desse aspecto evolutivo que um processo pode apresentar, Santos (2003) busca um modelo que permita a inovação na gestão de processos na organização. Ele explora a possibilidade de convergência entre os modelos de gestão por processos, como ABC (*Activity Based Cost*), ISO 9001, SIX SIGMA, e os modelos de gestão por níveis de

maturidade, como o CMM do Software Engineering Institute. A análise dos dois tipos de modelos mostrou sinergia e não divergências. Em sua conclusão (p. 13), diz que

> a gestão por maturidade parece ser o próximo passo dos modelos atuais de gestão por processos, uma vez que estes apesar de possuírem em muitos casos ferramentas para análise de melhoria contínua ainda carecem de maior definição sobre como verificar e acompanhar a evolução da organização no gerenciamento de seus processos.

A Figura 13 mostra um modelo de níveis de maturidade.

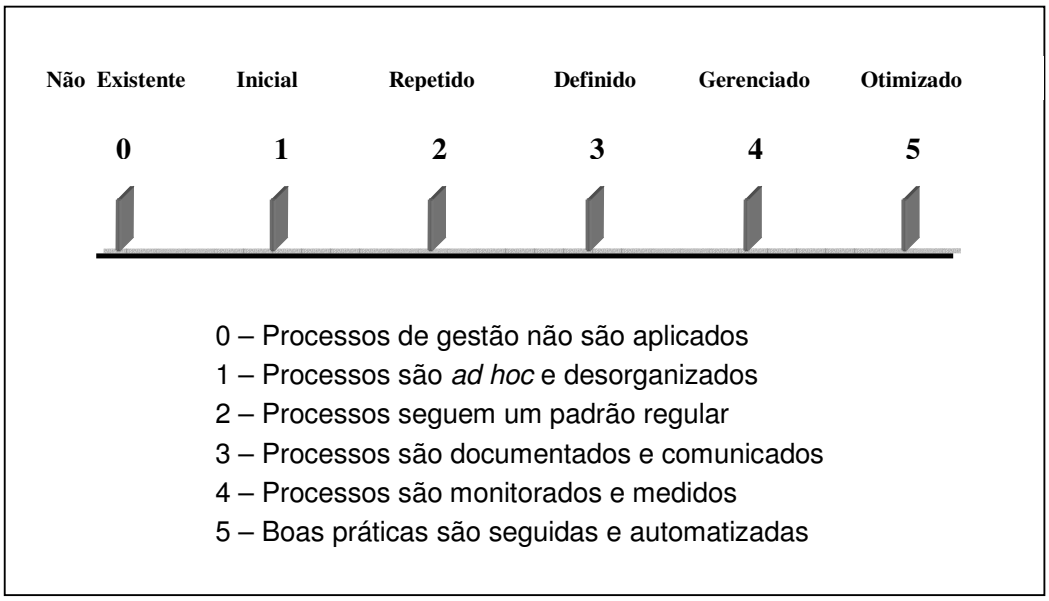


Figura 13 –Modelos de Maturidade (ITGI, 2007b, p. 18)

No COBIT, a modelagem de maturidade para gestão e controle sobre processos de TI é baseada no CMM, um modelo de maturidade desenvolvido pelo Software Engineering Institute (SEI) contendo boas práticas para avaliação e melhoria da maturidade nos processos de desenvolvimento de software. Através dos níveis de maturidade do modelo, são acrescentados atributos qualitativos de gestão, como: consciência e comunicação; políticas, planos e procedimentos; ferramentas e automação; habilidades e competência; responsabilidade e prestação de contas; e estabelecimento de objetivos e medidas de desempenho. O modelo genérico de maturidade especifica os seguintes níveis de maturidade:

0. **Não existente**: O processo não é reconhecido pela organização.
1. **Inicial:** A organização reconhece a importância do processo, contudo ele não é padronizado. As iniciativas são *ad hoc*, aplicadas individualmente. A gestão é desorganizada.
2. **Repetido:** O processo encontra-se em estágio onde procedimentos similares são seguidos por diferentes pessoas realizando a mesma tarefa. Não há treinamento formal ou comunicação de procedimentos padrões. A responsabilidade é individual. A confiança é depositada no conhecimento individual.
3. **Definido:** Procedimentos estão sendo padronizados, documentados, comunicados e treinados. Contudo, o indivíduo segue o procedimento por sua vontade.
4. **Gerenciado:** É possível monitorar e medir a conformidade a procedimentos e tomar medidas para sua correção. Processos estão continuamente sendo aperfeiçoados. Ferramentas são usadas de maneira fragmentada e limitada.
5. **Otimizado:** Processos foram refinados a um nível de melhores práticas, resultantes de contínuas melhorias. O fluxo de trabalho é automatizado, com ferramentas para melhorar a qualidade e eficácia, tornando a organização ágil para mudanças.

Guldentops *et al.* (2002) realizaram um *survey* para avaliar as maturidades de quinze processos do modelo COBIT, em empresas de diferentes continentes, tamanhos e setores. Foram obtidas 168 respostas válidas. As conclusões apontam para níveis médios de maturidade entre 2 e 2,5. Realizando alguns filtros, os resultados mostraram algumas diferenças, por exemplo em empresas grandes, do setor financeiro, ou multinacionais a média ficou entre 2,5 e 3. Em empresas do setor financeiro, particularmente, os processos de continuidade de serviços e de segurança de sistemas alcançaram os maiores níveis de maturidade, sendo parte desta explicação os eventos de 11 de setembro de 2001, segundo os autores. A comparação entre os continentes apontou para um nível maior de maturidade em empresas da Ásia e Oceania.

O referencial teórico-empírico apresentado nos itens anteriores deste segundo capítulo (Risco Operacional, Tecnologia da Informação e Governança) serviu de base para a criação do modelo conceitual da pesquisa, elaborado no terceiro capítulo.

Pôde-se perceber a importância da gestão de riscos, elemento de sustentação da governança corporativa. Em especial, foi apresentada a inovação nas recomendações do Basiléia II, referentes às boas práticas para gestão do risco operacional. A evolução das tecnologias de informação e comunicação e seu impacto nos processos internos das organizações foi comentado, bem como a sua relação com o risco operacional. Buscou-se, nessa revisão da literatura, apresentar também estudos de governança de tecnologia da informação, em especial do modelo COBIT, que indicam seu potencial de utilização na gestão de riscos operacionais.

A seguir, no último item desta revisão bibliográfica, o arcabouço teórico é completado com a referência à Teoria de Alta Confiabilidade.

2.4 Organizações de Alta Confiabilidade - OAC

O aumento do grau de complexidade pelas novas tecnologias nas organizações, em especial as TIC, levou teóricos desta área de estudo à busca de novas abordagens para compreensão de um conjunto de aspectos não contemplados anteriormente (BARLEY, 1986; ZUBOFF, 1988; WEICK, 2001 *apud* QUEIROZ e VASCONCELOS, 2004). Weick e Sutcliffe (2001) concordam que o estudo das organizações de alta confiabilidade[3] (OAC ou HRO - *High Reliability Organizations*) poderá contribuir para essa compreensão.

Há organizações que estão sujeitas a resultados catastróficos, mas conduzem operações relativamente livres de risco por longos períodos de tempo e tomam decisões consistentes que resultam em operações de alta qualidade e confiabilidade. Esse tipo de organização passou a ser estudada na Universidade da Califórnia, Berkeley, por teóricos como Todd La Porte e Karlene Roberts, em conjunto com outros pesquisadores como Charles Perrow, Richard Scott e Karl Weick, e passou a ser chamada de Organização de Alta Confiabilidade (BOURRIER, 2005).

Segundo Roberts (1990, p.101), a questão é a seguinte: "Quantas vezes a organização poderia ter falhado com conseqüências dramáticas?" e complementa: "Se a resposta para essa questão for muitas milhares de vezes, então a organização é altamente confiável." Exemplos

[3] Confiabilidade é a duração ou a probabilidade de desempenho livre de falhas sob determinadas condições (REASON, 1999 *apud* PINTO, 2005).

de organizações nesta categoria incluem usinas nucleares, empresas de aviação, refinarias de petróleo, serviços de emergência, controle de tráfego aéreo, operações militares e bancos, que operam em condições de alto risco devido às características de sua tecnologia ou das conseqüências sócio-econômicas que um erro pode provocar.

Alguns estudos recentes procuram investigar a aplicação da teoria acerca das OAC no campo da gestão de riscos operacionais – Eede e Walle (2005), Pinto (2005) , Eede *et al.* (2006) – e argumentam que seu embasamento é apropriado para estruturas teóricas na condução de gestão e análise de riscos.

2.4.1 Características

Neste estudo não se procura realizar ampla revisão bibliográfica da Teoria de Alta Confiabilidade, mas levantar as principais características de uma OAC para contribuir na avaliação da maturidade de processos de governança de TI, uma vez que estas organizações estão inseridas em um ambiente de alto risco e possuem habilidade para monitorar, detectar, prevenir e se antecipar a erros e falhas operacionais (WEICK e SUTCLIFFE, 2001).

Rijpma (1997 *apud* Eede *et al.*, 2006) mostra que os dois maiores determinantes desta tipologia organizacional são a complexidade de sistemas e o forte acoplamento. Sistemas complexos exibem interações complexas quando ele possui seqüências não planejadas ou inesperadas que não são visíveis ou compreensíveis imediatamente. Para Weick e Sutcliffe (2001), sistemas complexos trazem problemas de "gestão do inesperado". O Quadro 10 contrasta alguns atributos de sistemas complexos e sistemas lineares.

Quadro 10 – Sistemas Complexos *versus* Sistemas Lineares

Complexo	**Linear**
Proximidade de componentes	Segregação espacial, de componentes e sistemas
Conexões compartilhadas	Conexões dedicadas
Interconexão de sistemas	Segregação de sistemas
Substituições limitadas	Facilidade de substituições
Controles interativos múltiplos	Controles com propósitos simples
Limitada compreensão do processo tecnológico envolvido	Compreensão ampla do processo tecnológico

Fonte: Perrow (1994; *apud* Eede *et al.,*2006, p. 2)

Interdependência ou acoplamento refere-se ao grau de dependência mútua entre os componentes organizacionais, como aplicações, funções, departamentos ou indivíduos. Fraco acoplamento indica a possibilidade de operação independente entre os componentes, enquanto que um forte acoplamento conduz a uma troca contínua de informações, bens e serviços. A força do acoplamento influencia na quantidade de opções para recuperação em caso de falhas (Eede *et al.*, 2006).

O Quadro 11 mostra as diferenças técnicas entre os tipos de acoplamento.

Quadro 11 – Forte Acoplamento *versus* Fraco Acoplamento

Forte Acoplamento	**Fraco Acoplamento**
Processos sincronizados que não podem esperar	Esperas são permitidas
Processos em ordem precisa	Ordem ou seqüência podem ser alteradas
Somente um caminho para o resultado desejado	Substituições estão disponíveis
Rigidez de recursos – quantidade precisa e específica para a operação	Flexibilidade de recursos é possível, buffers e redundâncias estão disponíveis

Fonte: Perrow (1994; *apud* Eede *et al.,*2006, p. 3)

Eede *et al.* (2006) trabalham com algumas características consideradas como boas práticas nas OAC, como comunicação, tomada de decisão, cultura, aprendizagem e estrutura organizacional.

A comunicação variada provê meios para entendimento de papéis, responsabilidades e relacionamentos, e ainda o desenvolvimento de modelos mentais compartilhados entre os membros organizacionais. Como resultado, a autonomia e a interdependência entre membros do sistema se tornam explícitas e mais inteligíveis, provendo oportunidades para percepção e discussão de melhorias no sistema. Espaços de "não-punição" são providos para a diminuição de incerteza e análise de situações de falhas ou quase-falhas.

A tomada de decisão e a estrutura organizacional variam de estilos com regras e controles burocráticos a estilos de colegiado, em função das necessidades do ambiente e situações específicas. Em situações de emergência, observam Weick e Sutcliffe (2001, p. 16), as OAC "compartilham decisões na hierarquia e entre pares. Decisões são tomadas na linha de frente, e a autoridade migra para as pessoas mais experientes, independentemente de suas posições."

A cultura é uma outra variável organizacional considerada nas análises das OAC. É conceituada por Cook e Yanow (1993, *apud* Weick e Westley, 1996, p.364) como "um conjunto de valores, crenças e sentimentos, acompanhados dos artefatos de sua expressão e transmissão (tais como mitos, símbolos, metáforas, rituais) que são criados, herdados, compartilhados e transmitidos a um grupo de pessoas que, parcialmente, distinguem o grupo de outros grupos". Schein (1985) trata a cultura como um padrão de pressupostos básicos, inventados, descobertos ou desenvolvidos por um grupo, para lidar com problemas de adaptação externa ou integração interna, que têm funcionado suficientemente bem para serem considerados válidos e, desta forma, continuam a ser ensinados e compartilhados para novos membros do grupo como a maneira correta de perceber, pensar e agir em relação àqueles problemas. A validação e aceitação dos pressupostos básicos pelo grupo levam à consubstanciação desta crença em normas e procedimentos organizacionais.

Organizações que reconhecem que ainda têm algo a apreender possuem melhor chance de mitigar seus riscos. Compreender a possibilidade de falha é pré-condição para evitá-la. As OAC colocam grande ênfase na cultura para confiabilidade, e levam mesmo os pequenos

erros a sério, dando importância a pequenos sinais de ameaça. Essa cultura é construída em normas rígidas, com comprometimento em todos os níveis e troca de informações (Eede *et al.,* 2006).

Wishart e Elam (1996, *apud* Eede *et al.*, 2006) dizem que, com o objetivo de conquistar maior confiabilidade, concomitantemente a um alto grau de flexibilidade, as OAC tornam-se organizações de aprendizagem, ou organizações que aprendem.

Purser e Pasmore (1992, *apud* Weick e Westley, 1996, p. 366) trazem que as

> organizações de aprendizagem e de pensamento são sistemas de trabalho, intensivos em conhecimento, que se autodesenvolvem e também desenvolveram capacidades de se autodiagnosticarem, permitindo-lhes questionar os pressupostos e reavaliar suas relações com mudanças cambiantes do meio ambiente. (...) As organizações de trabalho, intensivas em conhecimento, 'aprendem a aprender' ao manter processos que examinam criticamente pressupostos, crenças, tarefas, decisões e problemas estruturais.

Weick e Westley (1996, p.369) analisam o oximoro entre organizar e aprender, identificando-os como processos antagônicos. "(...) o ponto de aprendizagem ótimo, tanto para o indivíduo como para a organização, está onde ordem e desordem se justapõem ou existem simultaneamente." Esses pontos representam a justaposição entre aprendizagem de *looping* único (adaptação, formação de hábito, redução de desvio, aprendizagem reativa, aprendizagem evolucionária) e de *looping* duplo (descoberta, exploração, aprendizagem pró-ativa, aprendizagem revolucionária).

Argyris e Schon (1978, *apud* Smith, 2001) descrevem os circuitos único e duplo de aprendizagem. No primeiro tipo de aprendizagem, as ações de detecção e de correção de desvios em relação a um determinado objetivo são operacionalizadas em função dos valores, planos e regras organizacionais estabelecidos, sem questioná-los. No segundo tipo, ocorre a fase de crítica das variáveis e estratégias institucionalizadas, o que pode levar a alterações no nível das variáveis de governo na organização, conforme a Figura 14.

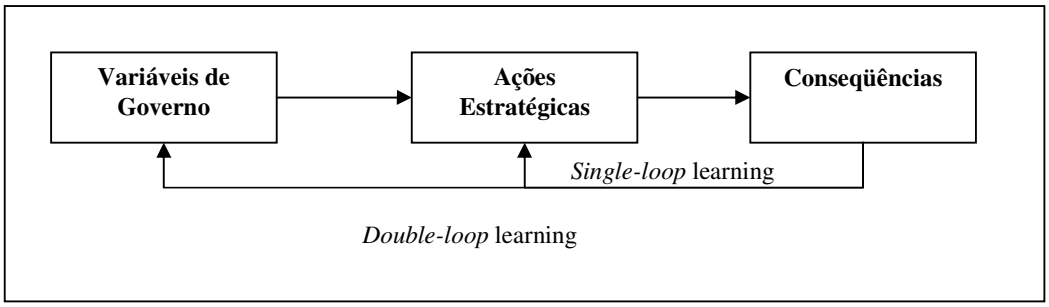


Figura 14 – Circuitos de Aprendizagem (Smith, 2001, p. 1)

Weick e Sutcliffe (2001) levantaram uma lista de características presentes em organizações de alta confiabilidade em seus processos de gestão de situações inesperadas. Constatou-se a preocupação constante com falhas, sejam grandes ou aparentemente pequenas, que podem coincidir em um determinado momento e trazer graves conseqüências. O relatório de situações de erros ou de quase erros é incentivado para promover aprendizado e há consciência da falibilidade de processamentos automáticos.

Outra característica de uma OAC diz respeito à busca de diagnóstico preciso e detalhado de situações, em contraposição à simplificação de interpretações, em virtude de seu ambiente complexo, instável, não conhecido completamente. Complementarmente, as OAC estudadas por Weick e Sutcliffe apresentaram-se hábeis na identificação prematura de falhas latentes, que consistem em imperfeições no processo operacional, como supervisão, comunicação de defeitos, procedimentos de segurança, treinamento, certificação e identificação de riscos. Esta detecção de falhas potenciais é realizada com forte atuação na linha de frente, preferencialmente no momento em que as anomalia são rastreáveis e podem ser isoladas.

As organizações de alta confiabilidade não são livres de erros, mas os erros não comprometem sua continuidade operacional e eficiência. Elas desenvolvem capacidades para detectar, conter e recuperar-se de erros. Nesse sentido, elas são organizações comprometidas com a continuidade do funcionamento das operações, demandando para isso profunda capacitação nas tecnologias de suporte aos seus processos e sistemas operacionais. A última característica apresentada refere-se à valorização da competência profissional, tornando as decisões colegiadas, evitando hierarquias rígidas, favorecendo a tomada de decisão na linha

de frente, com a autoridade migrando para as pessoas mais competentes, independentemente de seu posto.

O Quadro 12 resume as características apresentadas por organizações de alta confiabilidade, segundo Weick e Sutcliffe (2001).

Quadro 12 – Características de uma OAC

Característica	Descrição
Preocupação com falhas	Análise constante de todo tipo de falha e consideração de qualquer descuido como mau sintoma
Relutância em simplificar interpretações	Busca em compreender cada fase dento da complexidade de atividades e mantê-las separadas, de forma a permitir o controle e o gerenciamento
Sensibilidade aos procedimentos operacionais	Avaliação constante dos processos operacionais para identificar falhas potenciais
Compromisso com o funcionamento das operações	Estabelecimento de planos de contingência
Consideração a profissionais qualificados	Incentivo à tomada de decisão para solução de problemas entre os especialistas, independentemente de nível hierárquico

Fonte: Adaptado de Weick e Sutcliffe (2001, p. 10)

De acordo com Roberts (1990), os bancos estão entre as organizações de alta confiabilidade. A seguir, elabora-se o panorama geral do SFN, em especial do Banco Central do Brasil, lócus da análise deste estudo.

2.4.2 Sistema Financeiro Nacional

Assaf Neto (2005), Lemes Jr. *et al.* (2005) e Fernandes (2006) apresentam a estrutura do Sistema Financeiro Nacional (SFN), dividida em dois subsistemas: subsistema normativo e subsistema de intermediação. O subsistema de intermediação possibilita a transferência de recursos entre agentes econômicos – pessoas, empresas e governo – superavitários e deficitários.

Conforme Fernandes (2006), fazem parte do subsistema de intermediação: (i) as instituições financeiras *stricto sensu,* que captam depósitos à vista ou a prazo, obtêm recursos de repasses de outras instituições financeiras nacionais, estrangeiras ou do governo, além de conceder crédito; e (ii) as instituições equiparadas a instituições financeiras, com características híbridas do mercado financeiro e de capitais; (iii) as instituições não financeiras; e (iv) as instituições de atividades correlatas ao SFN. O Quadro 13 traz a classificação dessas instituições financeiras e respectivos órgãos de supervisão.

Quadro 13 – Participantes do Sistema Financeiro Nacional

Classificação	Tipo de Instituição (*)	Órgão Supervisor
Instituições Financeiras (IF)	Bancos Múltiplos (140) Bancos Comerciais (23) Banco de Desenvolvimento (4) Banco de Investimento (21) Caixa Econômica (1) Cooperativas de Crédito (1399) Sociedades de Crédito, Financiamento e Investimento (45) Sociedades de Crédito Imobiliário e Associações de Poupança e Empréstimo (18) Sociedades de Crédito ao Microempreendedor (41) Agências de Fomento (9)	Banco Central do Brasil (BCB)
Instituições equiparadas a IF	Sociedades de Arrendamento Mercantil (57) Sociedades Corretoras de Câmbio (43)	BCB
	Bolsas de Valores (1)	Comissão de Valores Mobiliários (CVM)
	Bolsas de Mercadorias e de Futuros (1) Sociedades Corretoras de Títulos e Valores Mobiliários (146) Sociedades Distribuidoras de Títulos e Valores Mobiliários (145)	BCB e CVM

Instituições não financeiras	Sociedades Administradoras de Consórcio (364) Administradoras de Sistemas de Liquidação e Custódia (CETIP, SELIC e outras) Correspondentes Bancários Agências de Turismo Credenciadas - câmbio	BCB
	Administradoras de Fundos de Investimento (5225)	CVM
	Sociedades Seguradoras Sociedades de Capitalização Entidades Abertas de Previdência Complementar Instituto de Resseguros do Brasil	Superintendência de Seguros Privados (SUSEP)
	Entidades Fechadas de Previdência Complementar	Secretaria de Previdência Complementar (SPC)
Instituições correlatas ao SFN	Sociedades de Factoring Administradoras de Cartão de Crédito	-

Fonte: Fernandes (2006, p. 8-50) e BACEN (2008)

(*) Quantidade de instituições, em 31/12/2003

As entidades supervisoras apresentadas no Quadro 13 compõem o subsistema normativo do SFN e têm os seguintes órgãos superiores: Conselho Monetário Nacional – atua junto ao BCB e CVM; Conselho Nacional de Seguros Privados – atua junto à SUSEP; e Conselho de Gestão de Previdência Complementar – atua junto à SPC.

O Banco Central do Brasil realiza atividades típicas de bancos centrais, tais como banco dos bancos (compulsório, redesconto), gestor do sistema financeiro (normatiza, autoriza, fiscaliza, intervém), agente da autoridade monetária (fluxo e liquidez), banco de emissão (moeda) e agente financeiro do governo (financia o Tesouro Nacional, administra a dívida pública e é depositário das reservas internacionais) (ANDREZO e LIMA, 2001).

Tendo como missão institucional assegurar a estabilidade do poder de compra da moeda e a solidez do Sistema Financeiro Nacional (BACEN, 2006b), a Diretoria Colegiada do Banco Central adotou, em 2002, três macroprocessos para cumprir seus objetivos estratégicos: (i) Formulação e gestão das políticas monetária e cambial, compatíveis com as

diretrizes do governo federal; (ii) Regulação e supervisão do Sistema Financeiro Nacional; e (iii) Administração do sistema de pagamentos e do meio circulante.

A gestão das políticas monetária e cambial é realizada pela Diretoria de Política Monetária (DIPOM) do Banco Central. A sua estrutura organizacional também é composta pelas diretorias: Diretoria de Administração (DIRAD); Diretoria de Assuntos Internacionais (DIREX); Diretoria de Estudos Especiais (DIESP); Diretoria de Fiscalização (DIFIS); Diretoria de Liquidações e Desestatização (DILID); Diretoria de Normas e Organização do Sistema Financeiro (DINOR); Diretoria de Política Econômica (DIPEC).

A DIPOM é formada por três unidades administrativas a seguir descritas (BACEN, 2006c):

Departamento de Operações Bancárias e Sistemas de Pagamentos – DEBAN

Este departamento possui como principal atividade o assessoramento à Diretoria na formulação e execução da política monetária e no estabelecimento de diretrizes para o Sistema de Pagamentos Brasileiro (SPB). Atua no sentido de elaboração de normas aplicáveis ao SPB, inclusive à Centralizadora da Compensação de Cheques e Outros Papéis (Compe). Busca, ainda, fornecer estudos para decisões sobre os recolhimentos compulsórios e operações de redesconto aos bancos.

Realiza o gerenciamento do Sistema de Transferência de Reservas (STR), núcleo do SPB que permite às instituições financeiras movimentar o saldo de suas contas de reservas bancárias junto ao Banco Central.

Departamento de Operações do Mercado Aberto – DEMAB

O Departamento de Operações do Mercado Aberto utiliza os instrumentos clássicos de política monetária para suas funções: as operações de mercado aberto de títulos públicos (*open market)*; as reservas compulsórias; e o redesconto. Executa, ainda, as operações de mercado aberto e outras aprovadas pela Diretoria Colegiada, assessora a gestão das políticas monetária e cambial, mantém o mercado de títulos públicos federais dinâmico e organizado, presta serviços ao Tesouro Nacional na administração da dívida mobiliária. O Sistema

Especial de Liquidação e de Custódia (Selic) é administrado pelo DEMAB. Este sistema realiza a custódia eletrônica dos títulos públicos federais.

A atuação do DEMAB no mercado se dá por meio de leilões públicos, negociando diretamente com os *dealers* credenciados semestralmente. A intervenção no mercado de títulos ocorre para que a taxa básica de juros – Selic – determinada como alvo pelo Comitê de Política Monetária (COPOM) aproxime-se ao máximo da taxa negociada no mercado.

Departamento de Operações das Reservas Internacionais – DEPIN

Este departamento tem como atividades principais o assessoramento e operacionalização da política cambial, a gestão tática do passivo externo e a administração das reservas internacionais do país. A gestão das reservas internacionais se dá por meio de um portfólio de referência, composto por títulos públicos soberanos de renda fixa e de alta liquidez, depósitos de moedas estrangeiras com contrapartes selecionadas, aplicações em ouro e aplicações de *money market*.

Com o objetivo de aperfeiçoar a gerência das reservas internacionais, em consonância com as melhores práticas adotadas internacionalmente, a Diretoria de Política Monetária definiu como ação prioritária os aperfeiçoamentos da modelagem de riscos, da avaliação de desempenho, do portfólio de referência, e do processo de investimento das reservas internacionais. Como órgão de assessoria nos estudos técnicos para a gestão eficaz dos riscos envolvidos em sua atividade, a DIPOM criou recentemente a Gerência-Executiva de Risco da Área de Política Monetária.

Encerra-se aqui a revisão de literatura desta dissertação. A incorporação, nos estudos de risco operacional, da área de conhecimento relativa às organizações de alta confiabilidade, enriquece os seus arcabouços conceituais, evidenciando aspectos pertinentes ao controle das complexidades ambiental, tecnológica e de sistemas, que resultam, nesse tipo de organização, na redução da probabilidade de ocorrência de falhas operacionais.

O próximo capítulo traz a metodologia do trabalho.

3 METODOLOGIA

Para a construção do conhecimento com validade científica, este trabalho seguiu a metodologia de pesquisa a seguir descrita.

3.1 Especificação do Problema

COMO A MATURIDADE NOS PROCESSOS DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO E AS CARACTERÍSTICAS DE ALTA CONFIABILIDADE CONTRIBUEM PARA A MITIGAÇÃO DO RISCO OPERACIONAL EM INSTITUIÇÕES FINANCEIRAS?

Diante da formulação do problema de pesquisa, foi selecionado para o estudo empírico um processo de negócio de uma instituição financeira. Buscou-se investigar a relação existente entre os processos de governança de tecnologia da informação (TI) e a mitigação de riscos operacionais, bem como a aplicabilidade de modelos de maturidade para a gestão desses processos. Por outro lado, também foi analisada a contribuição das características de alta confiabilidade, presentes no processo de negócio, para a mitigação de seus riscos operacionais.

O processo de negócio selecionado para a pesquisa foi o de redesconto bancário, conduzido pelo Banco Central do Brasil. Este processo está descrito no quarto capítulo.

3.1.1 Perguntas de Pesquisa

A partir dos objetivos propostos para esta pesquisa, as seguintes questões tornam-se importantes para a investigação empírica:

- Quais riscos operacionais podem ser identificados no processo de negócio selecionado?

- Qual o grau de contribuição dos processos de governança de TI para mitigação dos riscos operacionais encontrados?

- Qual a importância dos processos de controle de governança de TI para a mitigação dos riscos operacionais encontrados?

- Qual a aplicabilidade dos modelos de maturidade para a gestão dos processos de governança de TI?

- Quais os fatores de maturidade para governança de TI que podem ser considerados importantes nas organizações de alta confiabilidade?

3.1.2 Modelo Conceitual

Para explorar a relação entre processos de governança de TI e mitigação de riscos operacionais nesta pesquisa, elaborou-se o Quadro 14, em que são incluídos os processos selecionados no modelo COBIT e os respectivos referenciais teórico-empíricos que embasaram esta seleção, bem como o contexto de relevância relacionado às referências.

Quadro 14 – Processos de TI selecionados para a pesquisa empírica

Processo COBIT selecionado	**Referências**	**Relevância**
Avaliação e Gestão de Riscos de TI (PO9)	Quadro 6	Gestão de risco de TI
	Quadro 8	Gestão corporativa de riscos
Gestão de Projetos (PO10)	Quadro 7	Garantir a gerência de projetos
	Guldentops et al. (2002); Gerke e Ridley (2006) – Modelo COBIT	Processo avaliado como importante
Gestão de RH de TI (PO7)	BIS (2004), BACEN (2006) – Risco Operacional	Figura 1 – Componente "pessoas"
Asseguração da Continuidade de Serviço (DS4)	Quadro 6 Quadro 7	Garantia de continuidade de serviço
	Guldentops et al. (2002); Gerke e Ridley (2006) – Modelo COBIT	Processo avaliado como o 2º mais importante do modelo

Asseguração da Segurança de Sistemas (DS5)	Quadro 7	Garantir a segurança de sistemas
	Guldentops et al. (2002); Gerke e Ridley (2006) – Modelo COBIT	Processo avaliado como o mais importante do modelo
Gestão de Dados (DS11)	Quadro 7	Garantir a integridade e validade de dados
	Guldentops et al. (2002); Gerke e Ridley (2006)	Processo avaliado como o 4º mais importante do modelo
Avaliação e Monitoramento de Controles Internos (ME2)	Quadro 6	Auditoria interna de TI
	Donaldson (1990 *apud* Turnbull, 1997) - Governança Corporativa	Monitoramento
	Hawley e Williams (1996 *apud* Turnbull, 1997) Governança Corporativa	Controle
	NIST (2002) – Gestão de riscos	Controle
	COSO (1994), BIS (1998)	Controle interno
Promoção de Governança de TI (ME4)	OCDE (2004), BIS (2006) – Governança Corporativa	Estrutura, incentivos, objetivos estratégicos
	Meirelles et al. (2004), Albertin e Albertin (2005), Pinochet et al. (2005), Weill e Ross (2006) – Governança Corporativa e Governança de Tecnologia da Informação	Responsabilização, decisão

Fonte: O autor, a partir da revisão teórica

O Quadro 14 contém a relação dos oito processos de governança de TI selecionados, sendo os seis primeiros processos de tecnologia da informação, propriamente, e os dois últimos, processos de controle.

O primeiro processo do Quadro 14, denominado "Avaliação e Gestão de Riscos de TI", é intrínseco ao contexto desta pesquisa. Mostra-se relevante na maioria dos princípios do Basiléia II para gestão do risco operacional, conforme Quadro 6 (p. 50), e para a gestão corporativa de riscos, conforme os princípios nº 4 (avaliação de risco) e nº 8 (estrutura para controle e mitigação de risco) do Quadro 8 (p. 52).

A seleção do processo "Gestão de Projetos" fundamenta-se na análise de cenários de TI, conforme o Quadro 7 (p. 51), que demonstra a necessidade de assegurar a gerência de projetos de TI para reduzir as probabilidades de falhas em projetos de sistemas, e

conseqüentemente, de riscos operacionais. Os estudos de Guldentops *et al.* (2002) e Gerke e Ridley (2006) mostraram que este processo é visto como importante no modelo COBIT.

Já a seleção do processo denominado "Gestão de RH de TI" é baseada na própria definição de risco operacional, conforme BIS (2004) e BACEN (2006). O componente humano é um fator que agrega risco às operações de um processo de negócio, seja diretamente ou no suporte às operações, como é o caso dos profissionais da área de TI.

Por sua vez, o processo "Asseguração da Continuidade de Serviço" é salientado no princípio nº 7 (planos de contingência e continuidade de negócio) do Basiléia II, conforme Quadro 6 (p. 50) e também na análise de cenário referente a rompimento de serviços de TI, conforme Quadro 7 (p. 51). A evidência da importância deste processo para a governança de TI é corroborada nas pesquisas de Guldentops *et al.* (2002) e Gerke e Ridley (2006).

Segundo essas pesquisas, o processo "Asseguração da Segurança de Sistemas" foi avaliado como o mais importante do COBIT. A importância da segurança de sistemas também é levantada na análise de cenários do Quadro 7, em que atividades não autorizadas em sistemas ou a possibilidade de mau uso de informações sigilosas são fontes de riscos operacionais, demonstrando falha ou inadequação na segurança de sistemas.

Da mesma forma, o processo "Gestão de Dados" foi considerado importante por auditores e profissionais de TI. No Quadro 7, a garantia da integridade e da validade de dados em sistemas é fundamental para a eficiência da automatização, não permitindo resultados indesejados em função de falhas nas transações realizadas. Transações envolvendo recursos financeiros devem ser íntegras, não podendo ocorrer parcialmente, e devem ter seus dados armazenados em meios adequados e disponíveis.

A importância da implementação de controles para a mitigação de riscos levou à seleção do processo "Avaliação e Monitoramento de Controles Internos" para a pesquisa. A redução da probabilidade de uma ameaça valer-se de uma vulnerabilidade em um sistema é realizada por meio de medidas de controle, conforme Figura 7 (p. 44). O monitoramento de controles internos, atividade típica de auditoria, é salientado no segundo princípio do Basiléia II (Quadro 6, p. 50). Em COSO (1994) e BIS (1998) encontra-se que o processo de controle interno tem a eficácia e eficiência operacional como um de seus objetivos. Turnbull (1997)

consolida conceitos de governança corporativa, os quais apontam para a necessidade de monitoramento e controle para o alcance dos objetivos organizacionais. Portanto, esses atributos são da mesma forma relacionados à eficácia da governança de TI.

Finalmente, a inclusão no modelo conceitual do processo "Promoção de Governança de TI" está apoiada em OCDE (2004) e BIS (2006), que denotam a necessidade de desenvolvimento de uma estrutura para o estabelecimento de objetivos estratégicos, de recursos e incentivos adequados para a governança corporativa. Nessa direção, a governança de TI deve procurar o alinhamento estratégico para contribuir no alcance de objetivos da empresa, especificando os direitos decisórios e atribuindo responsabilidades, segundo Meirelles *et al.* (2004), Albertin e Albertin (2005), Pinochet *et al.* (2005) e Weill e Ross (2006).

O modelo conceitual proposto para este estudo é apresentado na Figura 15.

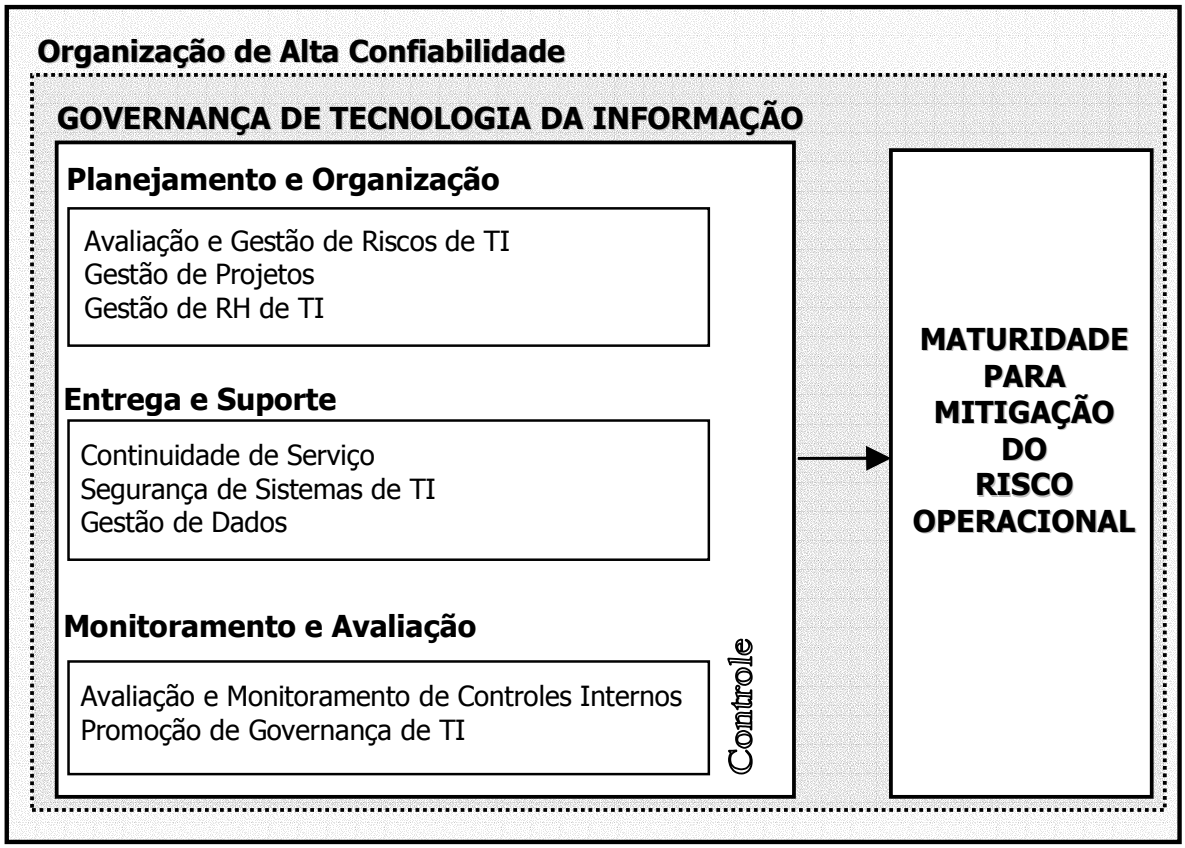


Figura 15 – Modelo conceitual proposto (o autor, a partir da revisão teórica)

Nesta pesquisa, as variáveis independentes são os processos de governança de tecnologia da informação, seus processos de controles e o contexto de alta confiabilidade, e a variável dependente é a maturidade para a mitigação do risco operacional.

Gil (1999) vê a existência de relações simétricas, assimétricas e recíprocas entre variáveis. Neste estudo o modelo indica a existência de uma relação assimétrica entre governança de TI em um ambiente de alta confiabilidade e maturidade para mitigação do risco operacional. Isto é, o modelo teórico captura a influência entre as variáveis.

A investigação teve abordagem predominantemente qualitativa, e conforme observa Creswell (2003), neste tipo de estudo o modelo pode servir como um guia para a pesquisa e questões a serem examinadas. A parte quantitativa do estudo adotou a estatística descritiva e a análise de freqüências para a investigação da contribuição dos processos de TI na mitigação de riscos operacionais. Para a comparação entre dois grupos de riscos operacionais identificados, foi realizado o teste não-paramétrico U de *Mann Whitney*, ao nível de confiança de 95%.

Contudo, não foi alvo de verificação empírica a força das relações causais. Assim, verificou-se o estabelecimento de relações entre as variáveis, porém não foram usadas medidas estatísticas para compreender as correlações entre elas.

3.1.3 Definição Constitutiva e Operacional das Variáveis

Kerlinger (1980) observa que o estudo de fenômenos e relações entre fenômenos não é possível sem a definição e o uso de diversas variáveis ou constructos, como são denominados nas ciências sociais ou comportamentais.

Assim, a "criação" de variáveis pelo pesquisador e a definição de como medir ou manipulá-las é uma etapa obrigatória no processo científico, uma vez que dão significado aos símbolos usados e esclarecem a escolha operacional adotada. Segundo Kerlinger (1980, p.46), "é como um manual de instruções para o pesquisador."

Faz-se, a seguir, a definição constitutiva (D.C.) e a definição operacional (D.O.) dos constructos que foram utilizados nesta pesquisa: risco operacional; processos de governança de TI e de controle selecionados para o estudo; maturidade; e alta confiabilidade.

Apesar da pesquisa ser predominantemente qualitativa, a definição constitutiva e operacional de variáveis facilita a compreensão e homogeneíza os conceitos. A pesquisa é exploratório-descritiva e busca entender a relação entre os processos de TI selecionados e a mitigação de riscos operacionais. A revisão da literatura permitiu a seleção de tais processos para o estudo, sem, no entanto, descrevê-los. A seguir, são apresentadas as suas definições constitutivas, as quais auxiliaram a confecção dos instrumentos de pesquisa citados nas definições operacionais dos processos de TI e de controle selecionados.

Risco Operacional

D.C.: Possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos. (BIS, 2004, p.137; BACEN, 2006, p.1).

D.O.: Os riscos operacionais foram explorados por meio de entrevistas focadas, em que se buscou compreender o processo de negócio (Anexo B) e riscos relacionados ao uso de TI (Anexo C).

Maturidade para Mitigação

D.C.: Maturidade refere-se à medida da intensidade do desenvolvimento da capacitação em um processo, isto é, quão bem o processo funciona (ITGI, 2007b). Mitigar significa reduzir para um nível aceitável as conseqüências ou probabilidade de um evento de risco adverso (PMBOK, 2000). Assim, a maturidade para mitigação de riscos, no contexto deste estudo, está relacionada ao desenvolvimento sucessivo de capacitações em processos de governança de TI para tornar mínimo o impacto de um evento de risco operacional.

D.O.: A maturidade dos processos de governança de TI e sua aplicabilidade são analisadas por meio de um simulador de maturidade e de perguntas abertas elaborados em um questionário eletrônico (Anexo F), e, ainda, por meio de entrevistas espontâneas focadas (Anexo D). Os modelos de maturidade que serviram de base para esta operacionalização são descritos no Anexo A.

Processos de TI: Avaliação e Gestão de Riscos de TI

D.C.: Processo de governança de TI que visa: a criação e manutenção de uma estrutura para gerenciamento de riscos; a documentação de níveis toleráveis de riscos de TI; a criação de estratégias de mitigação e riscos residuais aceitáveis; a identificação, análise e avaliação de impactos nos objetivos da organização por eventos não planejados; a divulgação e entendimento da avaliação de riscos pelos *stakeholders*, para permitir-lhes o alinhamento de riscos toleráveis, inclusive em termos financeiros (ITGI, 2007b).

D.O.: A contribuição do processo "Avaliação e Gestão de Riscos de TI" para a mitigação de riscos operacionais foi investigada por meio de questionário eletrônico, com escala intervalar do tipo Likert de 5 pontos (Anexo F). Para cada um dos riscos operacionais identificados, os respondentes informaram a importância deste processo de TI para a sua mitigação.

Processo de TI: Gestão de Projetos

D.C.: Processo de governança de TI que tem como objetivo: estabelecer uma estrutura para gestão de programas e projetos de TI; priorizar e coordenar os projetos; elaborar plano gerencial, de designação de recursos, aprovação de usuários, de planejamento de testes, de revisões pós-implantação para assegurar a gestão de riscos de projeto e entrega de valor para o negócio (ITGI, 2007b).

D.O.: A contribuição do processo "Gestão de Projetos" para a mitigação de riscos operacionais foi investigada por meio de questionário eletrônico, com escala intervalar do tipo Likert de 5 pontos (Anexo F). Para cada um dos riscos operacionais identificados, os respondentes informaram a importância deste processo de TI para a sua mitigação.

Processo de TI: Gestão de Recursos Humanos de TI

D.C.: Processo de governança de TI que tem como finalidade: identificar os requisitos de dados; estabelecer procedimentos para gestão de catálogos de dados, *backup* e recuperação de dados, e meios de armazenamento; garantir a qualidade, tempestividade e disponibilidade de dados (ITGI, 2007b).

D.O.: A contribuição do processo "Gestão de Recursos Humanos de TI" para a mitigação de riscos operacionais foi investigada por meio de questionário eletrônico, com escala intervalar do tipo Likert de 5 pontos (Anexo F). Para cada um dos riscos operacionais identificados, os respondentes informaram a importância deste processo de TI para a sua mitigação.

Processo de TI: Continuidade de Serviço

D.C.: Processo de governança de TI que tem por finalidade: criar, manter e testar planos de continuidade de serviço; utilizar *backup* para armazenamento de informações fora das instalações principais da organização; realizar treinamentos para a continuidade do negócio; assegurar a eficácia do processo de continuidade de serviço para minimizar a probabilidade de interrupção de serviços principais de TI para as áreas-chave de negócio (ITGI, 2007b).

D.O.: A contribuição do processo "Continuidade de Serviço" para a mitigação de riscos operacionais foi investigada por meio de questionário eletrônico, com escala intervalar do tipo Likert de 5 pontos (Anexo F). Para cada um dos riscos operacionais identificados, os respondentes informaram a importância deste processo de TI para a sua mitigação.

Processo de TI: Segurança de Sistemas de TI

D.C.: Processo de governança de TI que visa: gerenciar a segurança de sistemas; estabelecer papéis e responsabilidades para a segurança de TI, assim como políticas, padrões e procedimentos para a segurança; monitorar e testar periodicamente a segurança de sistemas; realizar ações corretivas para incidentes ou ameaças de segurança identificadas (ITGI, 2007b).

D.O.: A contribuição do processo "Segurança de Sistemas de TI" para a mitigação de riscos operacionais foi investigada por meio de questionário eletrônico, com escala intervalar do tipo Likert de 5 pontos (Anexo F). Para cada um dos riscos operacionais identificados, os respondentes informaram a importância deste processo de TI para a sua mitigação.

Processo de TI: Gestão de Dados

D.C.: Processo de governança de TI que visa: identificar os requisitos de dados; estabelecer procedimentos para gestão de catálogos de dados, *backup,* recuperação de dados, e meios de armazenamento; garantir a qualidade, tempestividade e disponibilidade de dados. (ITGI, 2007b).

D.O.: A contribuição do processo "Gestão de Dados" para a mitigação de riscos operacionais foi investigada por meio de questionário eletrônico, com escala intervalar do tipo Likert de 5 pontos (Anexo F). Para cada um dos riscos operacionais identificados, os respondentes informaram a importância deste processo de TI para a sua mitigação.

Processos de Controle: Avaliação e Monitoramento de Controles Internos

D.C.: Processo de controle de governança de TI que busca avaliar: a constituição do processo de monitoramento de controles internos; o monitoramento e informação de exceções de controle; resultados de auto-avaliações e revisões de terceiros; a eficácia na conformidade a leis e regulamentações (ITGI, 2007b).

D.O.: A relação entre o processo de controle "Avaliação e Monitoramento de Controles Internos" e a mitigação de riscos operacionais foi levantada por meio de entrevistas espontâneas focadas (Anexo D).

Processo de Controle: Promoção de Governança de TI

D.C.: Processo de controle de governança de TI para verificar: o estabelecimento de uma estrutura eficaz de governança de TI; a existência de papéis, lideranças, estruturas organizacionais, processos e designação de responsabilidades para garantir que os investimentos em TI estejam alinhados e haja entrega de serviços de acordo com os objetivos e estratégias organizacionais (ITGI, 2007b).

D.O.: A relação entre o processo de controle "Promoção de Governança de TI" e a mitigação de riscos operacionais foi levantada por meio de entrevistas espontâneas focadas (Anexo D).

Alta Confiabilidade

D.C.: Característica de organizações que operam em condições de alto risco devido à complexidade tecnológica ou das conseqüências sócio-econômicas que um erro pode provocar. Exemplos dessas organizações são usinas nucleares, empresas de aviação, refinarias de petróleo, serviços de emergência, controle de tráfego aéreo, operações militares e bancos (ROBERTS, 1990). Dois determinantes desta tipologia organizacional são a complexidade de sistemas e o forte acoplamento (RIJPMA, 1997 *apud* EEDE *et al.*, 2006). Complexidade denota a existência de seqüências não planejadas ou inesperadas, invisíveis ou incompreensíveis imediatamente. Acoplamento refere-se ao grau de dependência mútua entre os componentes organizacionais, como aplicações, funções, departamentos ou indivíduos.

D.O.: A investigação da tipologia e da presença de características de comunicação, cultura, tomada de decisão, estrutura e aprendizagem organizacional foi conduzida por meio de entrevistas espontâneas focadas (Anexo E).

3.1.4 Definição de Outros Termos Relevantes

Tecnologia

D.C.: O conjunto dos meios utilizados para o alcance de um resultado, um objetivo, um produto ou serviço é denominado tecnologia, que inclui as tecnologias mecânicas, como máquinas e equipamentos; as tecnologias humanas, como habilidades e energia física; e as tecnologias de conhecimento, que são significados e conceitos abstratos usados na produção (ROBERTS e GRABOWSKI, 1996). As tecnologias são de natureza sempre mutante, o que leva à sucessão de paradigmas tecno-econômicos que, por meio de inovações radicais e incrementais, geram as ondas largas de crescimento econômico (PEREZ, 2003), dentro de uma trajetória natural (NELSON e WINTER, 2002).

Tecnologia da Informação e Comunicação (TIC)

D.C.: Refere-se ao conjunto de tecnologias, como computadores e telecomunicações, que compõem o atual paradigma tecno-econômico. Surgiram após a inovação radical do microprocessador, no Vale do Silício, na década de 1970, e constituíram um novo estilo de produção, comunicação, gerenciamento e vida (CASTELLS, 1999). Fornecem suporte a múltiplos processos de negócio, muitas vezes criando redes interorganizacionais, com aplicações fortemente integradas, muitas vezes criando vulnerabilidades e riscos complexos (ROESSING, 2005).

Governança de Tecnologia da Informação

D.C.: É uma responsabilidade dos executivos e do conselho administrativo, e consiste em processos, estruturas e lideranças organizacionais que garantam que a tecnologia da informação sustente e estenda as estratégias e objetivos da organização (ITGI 2005).

Controle

D.C.: Processo no qual uma pessoa, grupo de pessoas ou organizações de pessoas determinam, isto é, intencionalmente afetam, o comportamento de uma outra pessoa, grupo ou organização (TANNENBAUM, 1975).

3.2 Delimitação e *Design* da Pesquisa

Abrangendo os quadrantes de paradigma funcionalista (positivismo) e interpretativo (BURRELL e MORGAN, 1979; NEUMAN, 1997; SAUNDERS et al., 2000) acerca das pressuposições epistemológicas, esta pesquisa teve como alvo o controle intersubjetivo para construção do conhecimento. Por um lado, buscou a objetividade no alcance de seus objetivos com base na teoria existente, e por outro lado permitiu explorá-la por meio de instrumentos de coleta de dados que foram úteis para a obtenção de *insights* para o estudo. Creswell (2003) não vê alternativa à interpretação pessoal na análise qualitativa de dados.

Buscando maior objetividade, com suspensão e distanciamento analítico, a pesquisa teve como metodologia a abordagem nomométicа à ciência social, com investigação baseada principalmente em protocolo sistemático. A natureza humana teve orientação predominantemente determinista, procurando não focalizar a autonomia comportamental dos indivíduos, mas as propriedades estruturais do contexto em que ocorre o fenômeno (BURRELL e MORGAN, 1979).

O fenômeno aqui estudado é o risco operacional proveniente do uso das tecnologias de informação e comunicação que apóiam a execução de um processo de negócio em uma instituição financeira.

3.2.1 Delineamento da Pesquisa

Delineamento, desígnio ou desenho refere-se, para Gil (2002, p.43), "ao planejamento da pesquisa em sua dimensão mais ampla, que envolve tanto a diagramação quanto a previsão de análise e interpretação de coleta de dados."

Para Yin (2005), a escolha de uma estratégia de pesquisa deve considerar três condições: (i) o tipo de questão de pesquisa; (ii) a extensão do controle que o pesquisador possui sobre eventos comportamentais atuais; e (iii) o grau de enfoque em acontecimentos contemporâneos ou históricos.

Assim, considerando-se a forma da questão-problema proposta nesta pesquisa, bem como a inexistência de controle, por parte do pesquisador, sobre o fenômeno, e ainda a focalização de eventos contemporâneos para o levantamento de dados, este estudo adotou a estratégia de pesquisa denominada estudo de caso, descrita por Yin(2005, p.32) como uma busca empírica que "investiga um fenômeno contemporâneo dentro de seu contexto da vida real, especialmente quando os limites entre o fenômeno e o contexto não estão claramente definidos." Neuman (1997) vê valor em um estudo de caso à medida que ele permite colher grande quantidade de informação em profundidade e buscar mais detalhes do caso a ser examinado.

Quanto aos meios, esta pesquisa é classificada como pesquisa bibliográfica, documental e de campo; quanto aos fins, a pesquisa é exploratória e descritiva, com análise predominantemente qualitativa de dados.

Gil (2002, p.41) descreve os critérios para classificação de pesquisa, dizendo que as pesquisa exploratórias "têm como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito e construir hipóteses [...] envolvem (a) levantamento bibliográfico; (b) entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado e (c) análise de exemplos". Ainda para Gil, as pesquisas descritivas têm como objetivo "a descrição das características de determinada população ou fenômeno ou, então, o estabelecimento de relações entre variáveis."

O método de pesquisa quanto ao uso da teoria é misto. Saunders *et al*. (2000) associam o método dedutivo ao teste de teorias, por meio de confirmação empírica de hipóteses, e o método indutivo ao desenvolvimento de teoria, resultante da coleta e análise de dados. Embora não tenha como objetivo o teste de hipóteses relacionadas ao referencial teórico de pesquisa, este trabalho descritivo-exploratório procurou, a partir da revisão teórica e com os achados de campo, tanto explorar a literatura existente para melhor compreender o fenômeno

quanto realizar “generalizações analíticas” (YIN, 2006 p.30) desta teoria, em um processo de criação de conhecimento.

Diante do problema de pesquisa formulado, o nível de análise escolhido foi o nível organizacional e a unidade de análise foi o processo de negócio de redesconto bancário. A coleta de dados teve corte transversal, contudo houve perspectiva longitudinal na análise de dados, uma vez que o fenômeno de risco operacional foi investigado a partir da reestruturação, em 2002, do processo de negócio estudado.

3.2.2 População e Amostra

Para Yin (2005), em um estudo de caso não pode ser considerada uma amostra. O estudo de caso não visa à generalização estatística, mas permite a generalização analítica em função do processo de imersão e na multiplicidade de fontes de evidências.

Os estudos de caso podem ser de caso único ou múltiplos. Para Yin (2005, p.63), “um (...) fundamento lógico para um caso único é o caso *representativo* ou *típico*”. As instituições financeiras do Sistema Financeiro Nacional podem ser consideradas como relevantes para a parte empírica desta pesquisa, por apresentarem processos de negócio tipicamente apoiados no uso da tecnologia da informação e também pelos esforços atuais de adequação ao Acordo da Basiléia.

Meirelles *et al.* (2005) evidenciam a necessidade de pesquisas empíricas em bancos centrais, que atuam como órgãos reguladores das instituições financeiras, e também como supervisores no segundo pilar do Basiléia II.

Desta forma, para a pesquisa empírica, ainda por razões de conveniência prática e de acesso a dados, optou-se por realizar a triagem de casos no Banco Central do Brasil, mais especificamente em sua Diretoria de Política Monetária, a qual possui responsabilidades inerentes à gestão das reservas internacionais, execução da política cambial, administração do sistema de pagamentos nacional e operações de mercado aberto, todas com grau considerável de complexidade operacional e que requerem alta confiabilidade.

A triagem foi realizada entre os dias 05 e 09 de novembro de 2007. Optou-se pela escolha do Redesconto Bancário como o processo de negócio para o estudo de caso.

A escolha levou em consideração os seguintes pontos: (i) a acessibilidade aos dados; (ii) a possibilidade de utilização de fontes complementares, em dois departamentos, para pesquisa empírica; e (iii) a dimensão e importância dos sistemas de tecnologia da informação que apóiam o processo de negócio.

3.2.3 Dados: Coleta e Tratamento

Para Gil (2002, p.43) "o elemento mais importante para a identificação de um delineamento é o procedimento adotado para a coleta de dados", sendo definidos dois tipos de delineamento: o que possui as ditas fontes de "papel" e o outro cujos dados são fornecidos por pessoas. Yin (2005) lista seis fontes de evidências para um estudo de caso: documentos, registros em arquivo, entrevistas, observação direta, observação participante e artefatos físicos.

As fontes de dados deste estudo, em sua maioria, foram entrevistas com informantes-chaves, incluindo profissionais das áreas de negócio, de tecnologia da informação e de auditoria interna. Também foram realizadas a pesquisa documental e a observação direta. Vergara (2006) lembra que os dados coletados devem ser correlacionados com os objetivos ou questões da pesquisa.

Desta forma, foram realizadas entrevistas, definidas por Yin (2005) como uma das mais importantes fontes para o estudo de caso. Os tipos de entrevistas utilizadas para a coleta de dados foram entrevistas espontâneas e focadas. Na entrevista espontânea, os informantes são indagados sobre sua opinião em um assunto, podendo sugerir outras pessoas como fontes de evidências. A entrevista focada caracteriza-se pelo período de duração da conversa, geralmente em torno de uma hora, assumindo um caráter informal, mas seguindo um conjunto de perguntas contidas no protocolo de estudo de caso (YIN, 2005).

Segundo Yin (2005, p. 92), um protocolo é "uma das táticas principais para aumentar a confiabilidade da pesquisa de estudo de caso e destina-se a orientar o pesquisador ao realizar

a coleta de dados a partir de um estudo de caso único". O ponto central do protocolo é o conjunto de questões que "formam a estrutura de uma investigação e não devem ser feitas literalmente ao entrevistado (p. 99)". Podem ser considerados como lembrete ao pesquisador à medida que os dados são coletadas e interpretados pelo pesquisador, que tem "a necessidade de equilibrar a 'adaptatividade' com *rigor* – mas não com *rigidez*" (p. 85).

Fontes múltiplas de evidências foram utilizadas, bem como o encadeamento de evidências, o que contribui para a validade de constructo, segundo Yin (2005). Ao todo, foram realizadas 14 entrevistas (Quadro 15) durante o período de 19 de novembro de 2007 a 1º de fevereiro de 2008. Com o consentimento dos entrevistados, elas foram gravadas[4] e posteriormente transcritas para realizar a análise de dados. O tempo médio de entrevista foi de 64 minutos.

Quadro 15 – Entrevistas realizadas

Número	Local	Data	Entrevistado	Protocolo
1	DEBAN	19-11-2007	Chefe de unidade I	Processo de negócio e Riscos Operacionais
2			Coordenador I	Processo de negócio
3		20-11-2007	Coordenador I	Processo de negócio
4			Coordenador I	Riscos Operacionais
5			Monitor	Processo de negócio e Riscos Operacionais
6		21-11-2007	Coordenador II	Alta Confiabilidade
7			Coordenador II	Riscos Operacionais
8		23-11-2007	Chefe de unidade II	Alta Confiabilidade
9	DEMAB	29-11-2007	Assessor Pleno	Processo de Negócio
10			Assessor Júnior I	Riscos Operacionais
11		30-11-2007	Coordenador III	Riscos Operacionais e Alta Confiabilidade
12			Assessor Júnior I	Riscos Operacionais
13	DEAUD	01-02-2008	Auditor I	Processos de Controle
14			Auditor II	Processos de Controle

Fonte: Pesquisa de campo

[4] Uma das entrevistas, gravadas em meio digital formato ".wav", apresentou problema de arquivo corrompido, o que impedia a sua audição. O problema foi corrigido por meio de um software de edição de arquivos binários.

Também foi desenvolvido, para a coleta de dados, um questionário eletrônico, com auxílio do banco de dados MS Access, para investigar a contribuição dos processos de TI na mitigação dos riscos operacionais identificados, simular o modelo de maturidade de processos e avaliar a sua aplicabilidade (Anexo F). O instrumento foi dividido em duas partes: a primeira para simular o modelo de maturidade dos seis processos de TI selecionados para o estudo; e a segunda parte para avaliar a contribuição desses processos de TI na mitigação de cada um dos riscos operacionais identificados. O respondente tinha a opção de deixar qualquer uma das duas partes em branco, caso não soubesse opinar.

Este instrumento de pesquisa foi respondido por uma amostra não-probabilística intencional ou por julgamento, contatada por correio eletrônico, com índice de retorno de 67% (8/12). A composição da amostra está no Quadro 16, constituída por profissionais do Departamento de Tecnologia da Informação (DEINF).

Quadro 16 – Amostra de Respondentes por Questionário Eletrônico

Número	Área	Opinou
1	Escritório de Projetos	Maturidade
2	Segurança de Sistemas	Maturidade e Mitigação de Riscos
3	Segurança de Sistemas	Maturidade e Mitigação de Riscos
4	Gestão de Dados	Mitigação de Riscos
5	Desenvolvimento de Sistemas	Mitigação de Riscos
6	Desenvolvimento de Sistemas	Maturidade
7	Infra-estrutura	Maturidade e Mitigação de Riscos
8	Infra-estrutura	Maturidade e Mitigação de Riscos

Fonte: Pesquisa de campo

Múltiplos métodos foram adotados para o tratamento dos dados, de acordo com os instrumentos de pesquisa e objetivos específicos traçados. Utilizou-se a análise de conteúdo para a descrição do processo de negócio, identificação de riscos operacionais, análise da importância dos processos de controle de governança de TI e avaliação da aplicabilidade de modelos de maturidade.

Foram utilizadas a estatística descritiva e análise de freqüências, com testes não-paramétricos, para a investigação da contribuição dos processos de governança de TI na

mitigação de riscos operacionais. Finalmente, para a investigação das características de alta confiabilidade, além da análise de conteúdo, foi adotada a técnica de mapa de associação de idéias, proposta nos trabalhos de Spink e Lima (2004, p. 107), para "sistematizar o processo de análise das práticas discursivas em busca dos aspectos formais da construção lingüística, dos repertórios utilizados nessa construção e da dialogia implícita na produção de sentidos" e de Vergara (2005, p.158): "dialogia refere-se a duas lógicas unidas, sem que a dualidade se perca nessa união".

A Figura 16 traz o *design* geral da pesquisa realizada.

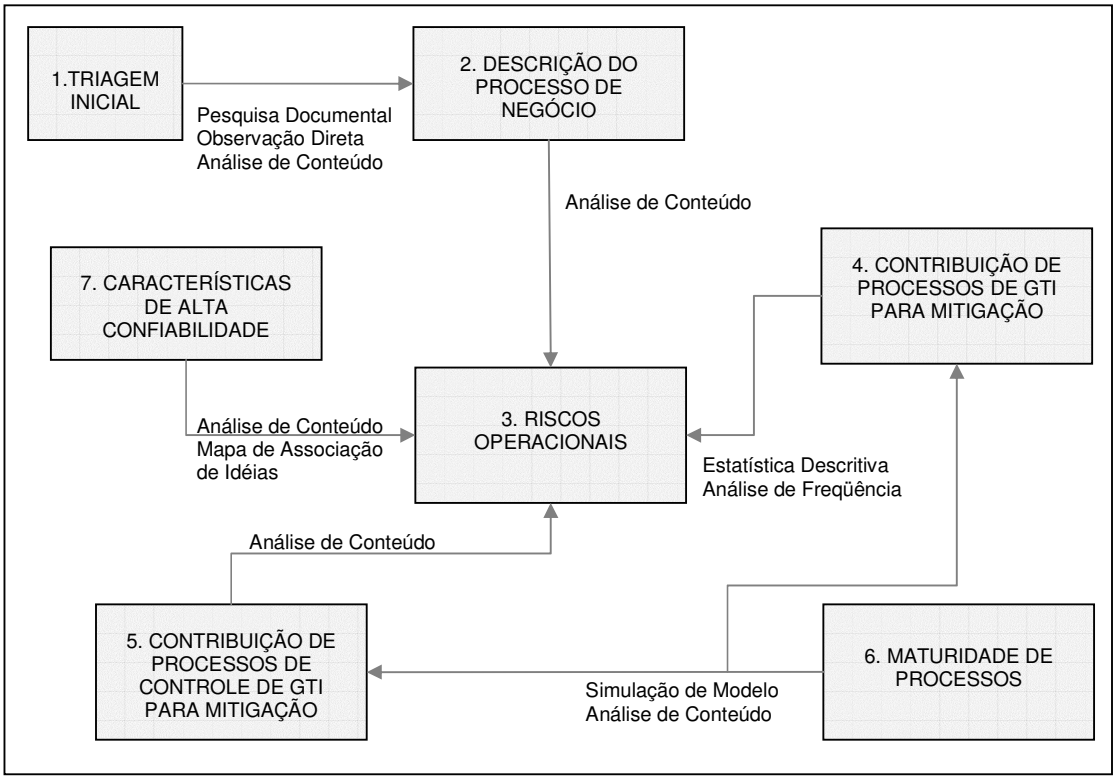


Figura 16 – *Design* da pesquisa

Após a triagem do estudo de caso, o processo de negócio foi descrito e os seus riscos operacionais foram identificados. Em seguida, foram verificadas as contribuições dos processos de TI e de controle para a mitigação dos riscos encontrados. A seguir, a gestão por maturidade de processos foi investigada, e, por último, a presença das características de alta confiabilidade pressupostas foram exploradas.

4 APRESENTAÇÃO E ANÁLISE DOS DADOS

Este capítulo tem por finalidade apresentar o relatório da pesquisa de campo, retomando o problema do estudo e os objetivos específicos que o compõe. A seguir, são apresentados o processo de negócio selecionado para a coleta de dados, os riscos operacionais identificados, a contribuição dos processos de governança de tecnologia da informação e seus controles para a mitigação desses riscos, a análise da gestão por maturidade e, finalmente, as características de alta confiabilidade percebidas.

4.1 Redesconto Bancário

O processo de negócio selecionado para a pesquisa de campo chama-se redesconto bancário, o qual representa, ao lado do recolhimento compulsório e das operações de mercado aberto, um dos instrumentos de administração da política monetária conduzida pelo Banco Central do Brasil (BCB).

Para descrever e explorar os riscos operacionais existentes no processo de redesconto bancário, foram realizadas entrevistas no Departamento de Operações Bancárias e Sistemas de Pagamentos (DEBAN), responsável direto pelo processo, e também no Departamento de Operações de Mercado Aberto (DEMAB). Outrossim, foram realizadas pesquisas documentais e observação direta das atividades nos sistemas. Nesta etapa da coleta de dados, foram realizadas nove entrevistas.

4.1.1 Descrição do Processo

A Circular BCB nº 3.105/2002 (BACEN, 2002), instituiu o Redesconto do Banco Central, cujo acesso "é restrito às instituições financeiras titulares de conta Reservas Bancárias" (Art. 1º), e suas operações podem ser "I - intradia, destinadas a atender necessidades de liquidez de instituição financeira, ao longo do dia; II - de um dia útil, destinadas a satisfazer necessidades de liquidez decorrentes de descasamento de curtíssimo prazo no fluxo de caixa da instituição financeira; III – de até quinze dias úteis (...); e IV – de

até noventa dias corridos (...)" (Art. 4º). A operação intradia de redesconto é definida como uma compra com compromisso de revenda, em que a compra e a correspondente revenda ocorrem no próprio dia. Para realizar essa operação, a instituição financeira deve possuir títulos públicos federais registrados no Sistema Especial de Liquidação e de Custódia (Selic), que integrem a sua própria posição de custódia (Art. 5º).

Antes de complementar a descrição do redesconto bancário, obtida por meio das entrevistas, a seguir é contextualizada a reestruturação do Sistema de Pagamentos Brasileiro, na qual o redesconto possui grande importância.

Com o objetivo de reduzir o risco sistêmico, o BCB reestruturou o Sistema de Pagamentos Brasileiro (SPB), que passou a liquidar, a partir de 22 de abril de 2002, as transferências interbancárias de fundos em um ambiente de processamento em tempo real, cujo núcleo é o Sistema de Transferência de Reservas (STR). Portanto, todas as operações de crédito ou débito na conta de reservas bancárias passam pelo STR, o qual não concretiza a operação na ausência de saldo nessa conta. Reservas bancárias são fundos em espécie, depositados no banco central pelos bancos, que são utilizados para obrigações de recolhimento compulsório, quando existir, e para liquidar pagamentos interbancários ou transações entre cada banco e o banco central (TORRES, 1999).

As operações com títulos públicos, realizadas no Sistema Especial de Liquidação e Custódia (SELIC), cuja administração é realizada pelo Departamento de Operações de Mercado Aberto (DEMAB), no Rio de Janeiro, também passaram a ser realizadas utilizando o conceito de liquidação em tempo real, o que permitiu a interligação entre o SELIC e o STR. Este último, operacionalizado no ambiente de processamento em Brasília.

Para realizar uma operação no SPB, as instituições financeiras participantes utilizam a infra-estrutura de mensageria. Foi criada a Rede do Sistema Financeiro Nacional (RSFN), para suportar o tráfego de mensagens entre os participantes. A RSFN é formada por duas redes de comunicação independentes, podendo sempre utilizar uma delas em caso de falha na outra.

Em decorrência dessa reestruturação no SPB, alterou-se o conceito de "dia de liquidação" para "hora de liquidação" das operações. Anteriormente, a liquidação das

operações era realizada no Banco Central ao final do dia, o que aumentava o risco sistêmico, pois havia risco de insolvabilidade no caso de a instituição financeira não disponibilizar os papéis lastro de operações realizadas. Esse foi um dos motivos para que em 2002 o BCB reestruturasse as operações do SPB.

Atualmente, as instituições financeiras organizam seus fluxos de caixa intradia para atender a uma grade de horário de funcionamento do STR. Esta grade define os horários de abertura e fechamento do sistema, bem como as faixas horárias ou "janelas de liquidação" dos pagamentos de câmaras, conforme a Figura 17.

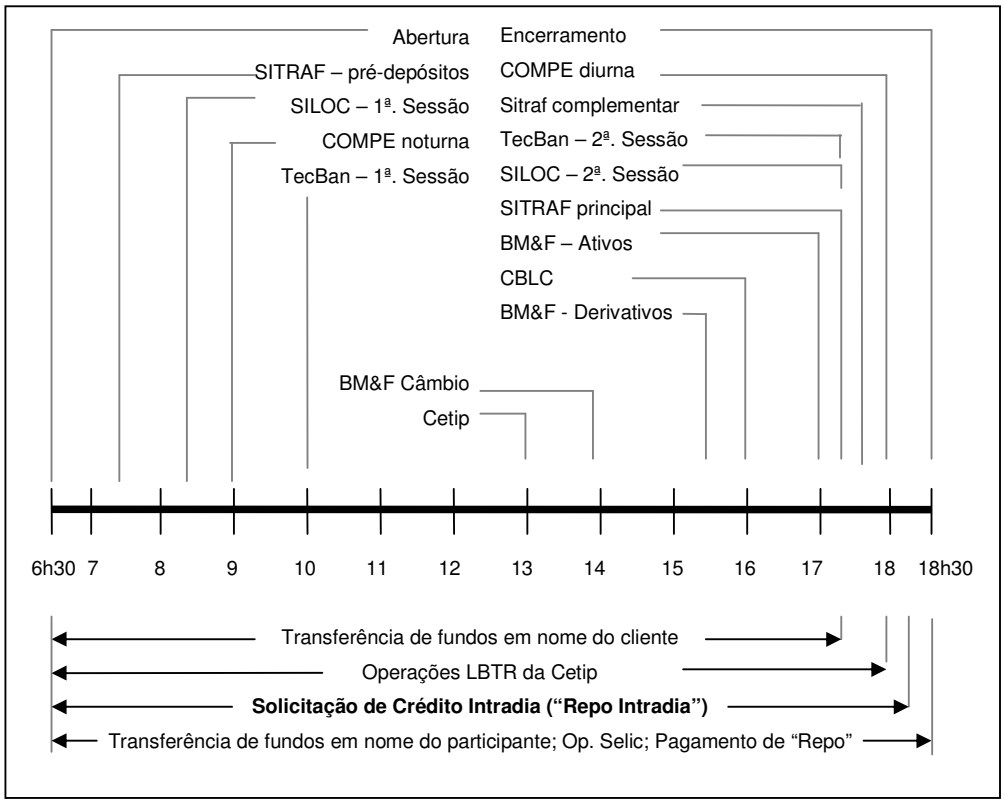


Figura 17 – Grade Horária do STR (BACEN, 2007b)

Em situação normal, o STR abre suas atividades às 6h30 e fecha às 18h30, nos dias úteis. Durante esse período, podem ser solicitados redescontos e também ocorrem diversas janelas de liquidação de pagamentos, mostradas no alto da Figura 17, em que as instituições financeiras com posição devedora nas câmaras devem autorizar, via mensageria, o respectivo débito em sua conta de reservas bancárias até o horário de encerramento de cada janela.

Entretanto, em busca de otimização de seus fundos, as instituições financeiras deixam, ao final de cada dia, suas reservas bancárias a um nível mínimo de recursos, uma vez que a respectiva taxa de remuneração é zero. Assim, não é incomum, logo na abertura da grade de funcionamento do STR, a necessidade de reservas bancárias para saques de meio circulante e para a realização de pagamentos e depósitos operacionais em câmaras do sistema de pagamentos, como o Sistema de Transferência de Fundos (SITRAF), que processa as transações de Transferência Eletrônica Disponível (TED) e o Sistema de Liquidação Diferida das Transferências Interbancárias de Ordens de Crédito (SILOC), que faz a liquidação de Documentos de Ordem de Crédito (DOC) e boletos de cobrança bancária. A Figura 18 apresenta as instituições financeiras participantes do SPB e os respectivos instrumentos financeiros.

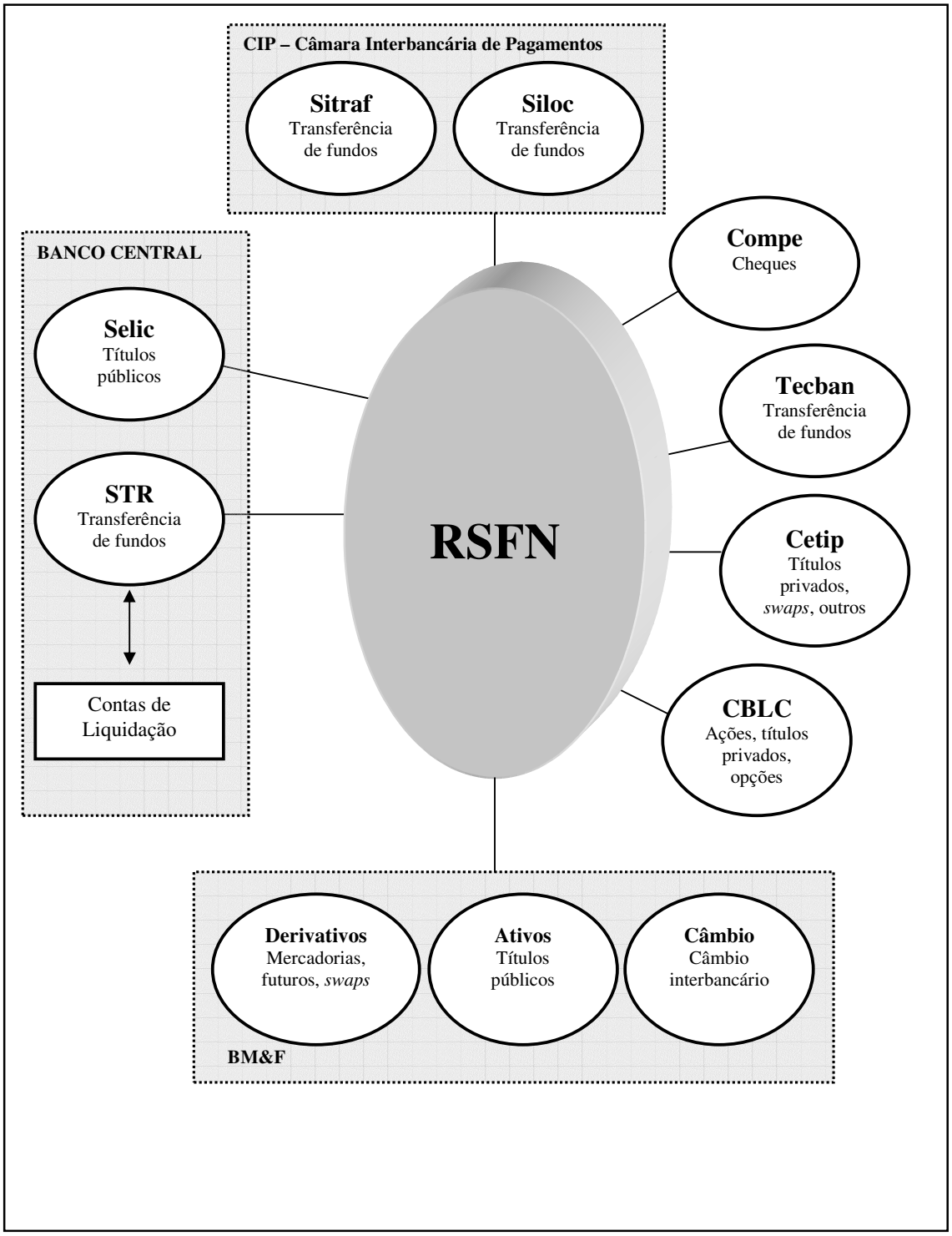


Figura 18 – Participantes do SPB (BACEN, 2007b)

Para realizar o ajuste de liquidez diária necessária no sistema de pagamentos, o banco central oferece facilidades de crédito (*standing facilities*), uma vez que não são permitidos saques a descoberto nas reservas bancárias. Para tomar recursos emprestados, as instituições financeiras realizam, então, operações compromissadas, em que apresentam títulos públicos de sua carteira para redesconto e recebem o valor respectivo, em reais, na sua conta de reservas bancárias. Observou-se, como exemplo, um banco que devia R$ 70 milhões em uma liquidação às 8h, e que recebeu o mesmo montante às 9h. Como esse banco não contava com reservas bancárias no início do dia, ele precisou do redesconto para atender ao fluxo de caixa negativo inicial.

Geralmente, as operações de redesconto são intradia, ou seja, a sua liquidação ocorre no mesmo dia da sua contratação. O BCB oferece, ainda, a opção de contratação de redesconto por um dia útil, cujo custo é calculado com base na taxa Selic mais 6 (seis) por cento. Os redescontos intradia não liquidados até o fechamento do STR são automaticamente convertidos para redescontos de um dia útil.

No Quadro 17, pode-se visualizar o volume de operações de redesconto bancário ou crédito intradia.

Quadro 17 – Operações de crédito intradia (média diária)

Ano/Mês	Quantidade	Valor total R$ milhões	Valor médio R$ milhões
2002	400	32.664,1	81,9
2003	389	26.465,0	67,9
2004	418	35.598,9	85,3

Fonte: BACEN, 2007b

A seguir, a operacionalização do redesconto bancário é descrita.

4.1.2 Operacionalização do Processo de Redesconto

Diariamente, as operações de redesconto somente estão disponíveis durante a grade de funcionamento do STR, das 6h30 às 18h30. Antes do horário da abertura, ocorre o processamento de pré-abertura do STR, que troca mensagens de sincronismo com o SELIC, em que ambos informam a sua prontidão para a efetiva abertura do sistema. Quando ocorre indisponibilidade em uma das partes, pode-se adiar o horário da abertura até que o problema seja sanado.

A operação de redesconto bancário, ou crédito intradia, é iniciada por meio de uma mensagem específica da instituição financeira, encaminhada ao Banco Central, como mostra a Figura 19. Existem várias modalidades de operação de redesconto, solicitadas por mensagens apropriadas, todas constando no Catálogo de Mensagens do SPB.

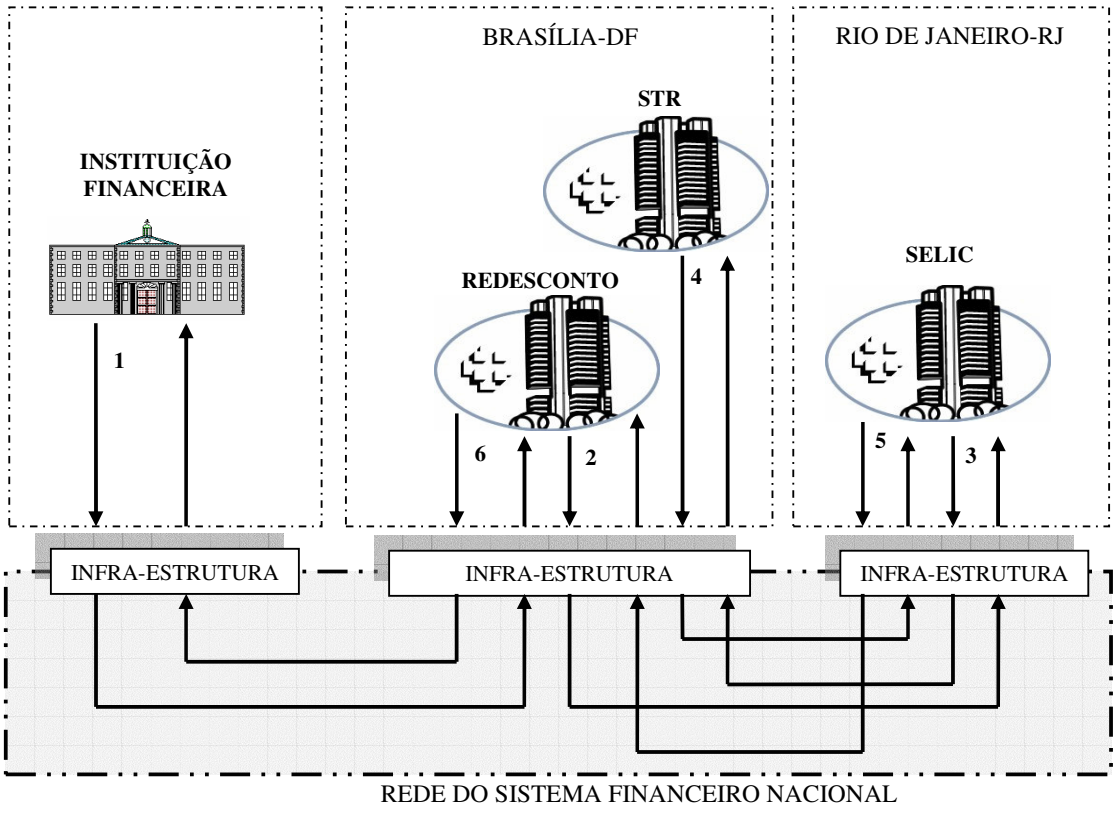


Figura 19 – Fluxo de mensagens da operação de redesconto (o autor, a partir da pesquisa documental)

Na Figura 19, percebe-se a participação de três grupos de serviços para a realização do redesconto, conforme o Quadro 18.

Quadro 18 – Grupos de Serviços do SPB envolvidos no redesconto

Nome do Grupo	Descrição
Redesconto (RDC)	Por meio destes serviços as instituições financeiras titulares de conta Reservas Bancárias têm acesso às operações intradia e de um dia útil, realizam consultas, liquidações e consolidação de várias operações de redesconto em uma única operação.
SELIC (SEL)	Por meio destes serviços, o participante da RSFN poderá comandar todas as operações com títulos públicos permitidas no Sistema Especial de Liquidação e de Custódia.
Sistema de Transferência de Reservas (STR)	O STR é o módulo responsável por executar transferências em tempo real no SPB.

Fonte: Catálogo de Mensagens do SPB (BACEN, 2007a)

Para possibilitar a realização do redesconto com títulos públicos, o SELIC calcula, diariamente, os preços unitários (PUs) de cada título, os quais são informados às instituições financeiras. A solicitação de redesconto (fluxo nº 1 na Figura 19) contém o título a ser usado como garantia na operação, bem como a quantidade de títulos necessária para o montante solicitado.

Antes de iniciar o fluxo nº 2 da Figura 19, o grupo de serviços de redesconto faz as validações iniciais da mensagem, que se encontra no padrão XML (*Extensible Markup Language*). O pedido de redesconto é identificado com um número identificador único, e uma nova mensagem é gerada para o SELIC.

No fluxo nº 3 da Figura 19, o SELIC informa a disponibilidade na carteira da instituição solicitante dos títulos entregues como garantia, os quais são então apartados, ficando em situação de pendência.

No fluxo nº 4, após creditar a conta de reservas bancárias da instituição financeira, o STR confirma a operação junto ao SELIC, que atualiza a situação dos títulos antes apartados e informa (fluxo nº 5) ao grupo de serviço de redesconto a concretização do crédito nas reservas bancárias e o bloqueio dos títulos no SELIC.

Finalmente, no fluxo nº 6, o solicitante recebe uma mensagem de resposta informando a finalização do processo. A mensagem de resposta pode ser uma mensagem de erro, caso tenha havido alguma falha no processamento ou não atendimento às condições para a contratação do redesconto.

O processo descrito acima se refere a uma contratação de redesconto. A maioria dessas operações contratas é liquidada no mesmo dia. Para isso, ocorre um fluxo semelhante ao descrito, porém na liquidação ocorre o débito na conta de reservas bancárias e os títulos são devolvidos à custódia da instituição financeira, no SELIC.

O envio de mensagens entre os participantes do SPB é realizado através de um software gerenciador de filas, que possui dados de controle para assegurar a entrega e retirada das mensagens das filas. Para trafegar na rede, as mensagens utilizadas no SPB são criptografadas e assinadas pelo emissor com sua chave privada. Os participantes devem registrar seus certificados digitais junto ao banco central, que os disponibiliza para os demais participantes, para que, de posse da chave pública do emissor, o destinatário possa processar a mensagem recebida.

Para efetivar uma contratação de redesconto é necessário atender aos requisitos do modelo 1 de liquidação "Entrega Contra Pagamento" (*Delivey Versus Payment-DVP*), que oferece um mecanismo que assegura que a entrega ocorre se, e somente se, o pagamento ocorrer, isto é, o crédito nas reservas somente acontece após a confirmação da disponibilidade do título público. Antes da implantação do SPB, utilizava-se o modelo 2 DVP (BIS, 1992). Os pagamentos ocorriam somente ao final do dia, o que tornava possível uma operação a descoberto nas reservas bancárias, aumentando o risco sistêmico no Sistema Financeiro Nacional. A alteração para o modelo DVP 1 foi um dos principais pontos da reestruturação do sistema de pagamentos do país.

Se a instituição financeira apresentar problemas técnicos em seu ambiente, ela pode recorrer ao sistema de contingência, nas modalidades integral ou parcial. Na contingência integral, o participante utiliza o sítio do banco central, após ser autorizado pela equipe de monitoramento do SPB, e gera as mensagens necessárias, com o uso de chaves de segurança. Na contingência parcial, o participante é atendido por telefone pela equipe de monitoramento, que insere as operações solicitadas.

Cada instituição financeira possui uma espécie de fila seqüencial por onde trafegam suas mensagens de redesconto, além das outras mensagens que tenham impacto na conta de reservas bancárias. A fila implementa o conceito "FIFO" (*Firt in first out*), o que impede a processamento concomitante de solicitações de redesconto. Por outro lado, existe uma fila de processamento paralelo em que são colocadas as mensagens apenas de consulta.

A operacionalização do processo é suportada por equipes de monitoramento, tanto das áreas de negócio quanto das áreas de tecnologia da informação, que realizam suas atividades da pré-abertura ao fechamento dos sistemas.

4.1.3 Riscos Operacionais no Processo de Redesconto

A identificação dos riscos operacionais teve como foco o componente da tecnologia da informação enquanto suporte para o funcionamento do processo de negócio de redesconto bancário.

A automatização, em todos os participantes do SPB, é alta. A afirmativa de Roessing (2005, p.4), no sentido de que a otimização e remoção de *buffers* entre os processos concentra os riscos no ambiente de TI, foi corroborada nas entrevistas: "A mensagem chegou aqui ela vai passar automático (...) A gente não tem que intervir em nada (...) A nossa parte é toda automatizada (...) Logo quando o sistema entrou, a gente tinha muito, mas muitos erros no redesconto. Eu acho que a partir de uma determinada etapa as instituições procuraram automatizar o redesconto. Ele provavelmente só diz qual é o título e o sistema faz o resto" (Resp. 7).

Assim, para a identificação dos riscos operacionais relacionados ao processo de negócio, foram levantadas, por meio da análise de conteúdo, as falhas potenciais de sistemas de informação e de infra-estrutura que poderiam comprometer o ciclo de processamento demonstrado na Figura 19 (p. 96). Em seguida, buscou-se a triangulação de dados para confirmar a existência desses riscos operacionais.

A principal dificuldade para o alcance deste objetivo foi que a maioria das falhas identificadas, durante a análise do processo de negócio, não constitui, na visão dos entrevistados, risco operacional na atualidade. Constantemente, recorria-se à visão de hipóteses de riscos operacionais, pois os sistemas envolvidos no processo estão estáveis, e as falhas cotidianas são raras: "Essa possibilidade foi exaustivamente testada (...) Olha, é... isso é uma das coisas mais improváveis de acontecer" (Resp 7).

Desta forma, buscou-se identificar os riscos operacionais passíveis de ocorrer, mesmo que já mitigados durante o projeto, desenvolvimento e testes dos sistemas no ambiente de homologação, em que participaram todas as instituições financeiras, realizando testes de desempenho e funcionalidades dos sistemas.

Neste contexto, pôde-se observar a existência de dois tipos de riscos operacionais: (I) os presentes na rotina diária do processo de negócio, já observados ao menos uma vez; e (II) os risco operacionais pouco prováveis, circunstanciais ou hipotéticos. Estes últimos, após mais de cinco anos de funcionamento do SPB, já estão mitigados, sendo pela implementação de controles ou pela baixa probabilidade de vulnerabilidades e ameaças.

Mesmo assim, todos eles foram identificados, para possibilitar a avaliação da contribuição dos processos de governança de TI na sua mitigação, à época da implantação do sistema.

Na rotina diária do processo de negócio, observou-se como um dos principais riscos operacionais a comunicação entre os grupos de serviços utilizados na operacionalização do redesconto bancário, principalmente a comunicação entre o Sistema de Transferência de Reservas (STR), localizado em Brasília, e o SELIC, localizado no Rio de Janeiro: "A ligação hoje é quase que umbilical (...) Hoje é em tempo real. Se o STR pára, o Selic não consegue

liquidar nada, a não ser o que for movimento extra reserva bancária. Ele quase pára. Se o Selic pára, eu não paro, mas grande parte das minhas operações depende do Selic" (Resp 1).

Dada a importância da disponibilidade dos grupos de serviços para o bom funcionamento do processo de redesconto, foi institucionalizado o procedimento de pré-abertura dos sistemas, que trocam mensagens de prontidão entre si antes da abertura, realizada às 6h30. Em 2002, com a indisponibilidade do grupo de serviços do SELIC, foi necessário abrir o sistema, mesmo após a prorrogação de abertura para as 8h. "É um caos? É! (...) As instituições terão problema de liquidez durante o dia. Não vão honrar seus pagamentos. Dependem do crédito intradia" (Resp 4).

Ainda na rotina diária, o arquivo contendo os títulos públicos com preços respectivos para redesconto deve ser disponibilizado para os participantes. Todos os títulos públicos colocados no mercado primário pela mesa de operações do DEMAB, sejam por Leilão Formal ou Leilão Informal, têm seus preços informados para as operações compromissadas com o Banco Central. Este arquivo é gerado pelo Sistema Especial de Liquidação e Custódia e encaminhado para Brasília, diariamente, que o coloca em seu sítio na Internet. Outra forma de acesso é por meio de mensagem, em que o participante consulta os preços unitários (PUs). Existe, como terceira opção, a possibilidade de obter os PUs no sítio da Associação Nacional das Instituições do Mercado Financeiro (Andima), que auxilia o DEMAB na administração do SELIC. Neste processo, vê-se também a automatização e sua dependência: "A instituição procura automatizar ao máximo o seu processo, ela vai automaticamente buscar essas informações na página do BC na Internet (...) Uma instituição entrou com pedido de redesconto para um desses títulos que não existia PU e o sistema dava erro porque não tinha esse título. Foi necessário recarregar o arquivo ao longo do dia. Risco operacional é altíssimo" (Resp 4).

Observou-se que a duração de uma contratação de redesconto é realizada, em média, em 4 (quatro) segundos. Contudo, durante a rotina diária, este desempenho pode ser afetado, ocasionado por fatores geralmente de infra-estrutura: "Teve uma vez, em 2005, uma crise chamada síndrome das 5. Eram 10 para as 5 (17h) o telefone começava a tocar, o participante estava com problema. Simplesmente a máquina parava. Atingia os 100%." (Resp 4). Para auxiliar as equipes de monitoramento dos sistemas, há softwares específicos para rastrear as etapas do processamento. Casos de exceção no processamento são identificados, desde a

recepção das mensagens (fluxo nº 1 da Figura 19, p. 96) até o envio das respostas aos participantes (fluxo nº 6 da mesma figura).

Se houver problemas técnicos no ambiente de tecnologia da informação do participante, que lhe cause a impossibilidade de solicitar o redesconto, a sua falta de liquidez poderá comprometer a liquidação dos resultados líquidos apurados nas câmaras existentes no SPB. A liquidação dos saldos de cada participante das câmaras deve ser realizada nas reservas bancárias, de acordo com suas grades horárias de liquidação. "Se você não disponibiliza redesconto, ou você vai ter que postergar aquela grade ou vai colocar a instituição em uma situação de inadimplência" (Resp 5).

Ao solicitar um redesconto, o participante aguarda a mensagem de resposta do Banco Central informando-lhe o respectivo crédito em sua reserva bancária, para então sensibilizar seus controles internos. Se essa resposta não é encaminhada, em instantes o participante entra em contato com a equipe de monitoramento para solicitar esclarecimentos. "O piloto da reserva do banco liga e você vai olhar na reserva dele e já está lá o crédito. Aí você vai correr atrás do problema. Aí se ele está agoniado para fazer um pagamento, a gente avisa, olha pode fazer que o dinheiro já está na sua reserva. Assim que o problema for solucionado você vai receber a resposta" (Resp 5).

Além da interdependência entre os grupos de serviços RDC, STR e SELIC para o processamento do redesconto bancário, existem também interfaces com outros componentes, como o responsável pela contabilização das transações. "Teve uma falha grave no contábil, que ficou indisponível. O STR funcionava, mas ele não funcionava. Com isso, os pagamentos que o BC tinha que fazer, não conseguia. Os nossos lançamentos passam pelo contábil antes de sair" (Resp 7).

Todo o fluxo de mensagens é registrado em um Sistema Gerenciador de Banco de Dados (SGBD). Este recurso também é intensamente utilizado e sua disponibilidade é um fator crítico para a operacionalização do processo de negócio: "Teve uma falha grave. O banco de dados teve uma pane. Ficou parado um tempo. Virou um caso de estudo para a IBM" (Resp 7).

A última atividade da rotina diária consiste em realizar o fechamento dos sistemas, de acordo com a grade horária prevista. A condição para isso é que não exista nenhuma mensagem pendente de processamento. Em uma situação extrema, o fechamento é realizado mesmo nessa situação em virtude das interfaces existentes com outros sistemas: "O limite é 23h59. Se não tiver voltado até esse horário, vai fechar com o que tiver (...) Os bancos não iriam conseguir fechar o sistema com outra data. A contabilidade fecha à meia-noite (sistemas)" (Resp 7).

A seguir, o Quadro 19 consolida os riscos operacionais identificados na rotina diária.

Quadro 19 – Riscos Operacionais Tipo I - Rotina Diária

Nº	Risco Operacional	Descrição
1	A contratação ou liquidação de um redesconto é processada parcialmente	Durante o fluxo da operação de redesconto ocorre alguma falha que leva à interrupção do processo, deixando-o incompleto
2	As informações de pré-abertura provenientes do Selic não são disponibilizadas corretamente, o que poderá adiar a abertura do Grupo de Serviço de Redesconto	A condição necessária para a abertura dos sistemas é a realização do sincronismo entre eles, no procedimento de pré-abertura. A grade de abertura é prevista para as 6h30, sendo que se pode prorrogar a abertura, se julgado conveniente
3	Há indisponibilidade dos Grupos de Serviço de Redesconto ou STR	Os grupos de serviços RDC e STR são fundamentais para a concessão de redesconto bancário. Trocam mensagens entre si e com o Selic para a efetivação do processo
4	Há indisponibilidade no sistema Sisbacen, ocasionando falha na contabilização de redescontos	A interface com o componente contábil incrementa o risco no processamento de um redesconto bancário
5	O banco de dados torna-se indisponível	Todas as transações processadas pelos grupos de serviço devem ser armazenadas por um sistema gerenciador de banco de dados
6	O Grupo de Serviços de Redesconto é iniciado sem que todos os sistemas envolvidos estejam prontos (STR, Selic e outros)	A abertura sem todos os grupos de serviço pode levar ao acúmulo de mensagens a processar, o que ocasionará transtorno na comunicação entre os participantes e o Banco Central
7	Ocorre falha de comunicação com o Selic, que torna inoperante o processo de redesconto	O canal de comunicação entre o Selic e os demais grupos de serviço, se indisponível durante o dia, poderá levar à situação de falta de liquidez nos pagamentos do SPB devido à ausência da assistência de crédito intradia

8	Os redescontos não são processados com desempenho adequado devido à limitação de recursos de infra-estrutura	Com a reestruturação do SPB, o processamento das mensagens ocorre em tempo real, e o desempenho do processamento deve ser adequado
9	Os títulos para redesconto estão com erro de cálculo de Preço Unitário (PU)	Os preços das operações compromissadas com o Banco Central são informados diariamente para os participantes, para todos os títulos públicos existentes no mercado. A inexatidão desses dados poderá criar exposição a risco de crédito
10	Participante (Instituição Financeira) não consegue enviar mensagem de redesconto para o Banco Central	Um problema no ambiente tecnológico do participante ou do Banco Central pode comprometer o processo de redesconto e conseqüentemente a liquidação dos resultados líquidos das câmaras no STR
11	Participante não consegue obter Preços Unitários (PU) de títulos públicos para redesconto	Para solicitar o redesconto, a instituição financeira deve especificar qual o título e quantidade que será dada como garantia para o Banco Central. Para isso, é imprescindível o acesso do participante ao arquivo de PUs
12	Participante não consegue reordenar ou revogar redescontos pendentes, por exemplo, quando solicita redesconto maior que sua disponibilidade de títulos para redesconto	Quando o participante solicita redesconto e não possui a quantidade de títulos em custódia, o Selic aguarda, por um tempo determinado, a disponibilidade da quantidade total solicitada. O participante deve aguardar o término desse processamento para alterar ou cancelar a sua solicitação
13	Participante não recebe resposta de sua mensagem de sua solicitação de contratação ou liquidação de redesconto	A sensibilização interna nos sistemas do solicitante de redesconto é muito importante para que ele possa prosseguir sua atividade de controle de fluxo de caixa
14	Sistema não consegue fechar o dia devido à existência de mensagens pendentes	O encerramento dos grupos de serviços do SPB é realizado ao final do dia, e o processamento de todas as mensagens recebidas deve estar concluído
15	Sistema não reconhece o título solicitado para o redesconto, sendo que ele é válido	O arquivo com os títulos públicos deve estar completo, com todos os papéis emitidos no mercado primário
16	Uma mensagem de pedido de redesconto não é disponibilizada tempestivamente ao Grupo de Serviços de Redesconto	Para que o tempo de processamento seja adequado, todos os componentes de tecnologia da informação envolvidos no processamento das mensagens de redesconto devem estar em pleno funcionamento e com desempenho adequado

Fonte: Dados de pesquisa

Na categoria dos riscos operacionais circunstanciais, por sua vez, aparecem as falhas potenciais de baixa ou baixíssima probabilidade, nunca observadas, mas que podem ter um

alto grau de impacto na avaliação de riscos. O Quadro 20 mostra a relação de riscos operacionais desta categoria.

Quadro 20 – Riscos Operacionais Tipo II – Circunstanciais ou Hipotéticos

Nº	Risco Operacional	Descrição
17	A criptografia das mensagens de redesconto é quebrada	Para a segurança do sistema, as mensagens são criptografadas e assinadas pelo emissor
18	A diversidade das regras do negócio torna complexa a implementação e alta a probabilidade de defeitos de software	A complexidade tecnológica e das regras do processo de negócio pode levar ao desenvolvimento de produtos instáveis ou de difícil manutenção
19	A existência de certificados digitais vencidos ou desatualizados impede a troca de mensagem	Anualmente é realizada a troca de certificados digitais e das chaves pública e privada. Para isso, os participantes devem atualizá-los no SPB antes da expiração do certificado vigente
20	Há indisponibilidade no acesso de contingência (internet)	O acesso de contingência é um recurso que as instituições têm para continuar suas operações via mensageria, mesmo que seus sistemas ou infra-estrutura apresentem problemas técnicos. Como alternativa para o funcionamento do SPB existe a alternativa de entrada em contingência do participante, que é devidamente autorizada pelo BC
21	O atendimento a novos requisitos ou demanda pontual no sistema é intempestiva	Eventuais mudanças nas regras do processo de negócio podem demandar alterações tempestivas nos sistemas
22	O componente de software implementado não atende aos requisitos de desempenho e de flexibilidade para incorporar inovações tecnológicas	A codificação dos requisitos de um sistema em linguagens de programação gera componentes de software, os quais devem responder às necessidades de desempenho satisfatório, bem como permitir que inovações no ambiente de TI (hardware e software) possam ser utilizadas para a evolução do sistema
23	O desempenho do sistema é degradado devido a ações maliciosas	Ameaças intencionais, ou mesmo não intencionais, podem degradar o desempenho de um sistema, como a ativação de muitos processos concorrentes para processamento em níveis altos de prioridade ou a indisponibilidade de recursos
24	O processamento de redesconto gera uma inconsistência de dados	Uma operação de redesconto deve gerar dados íntegros após a sua realização. Por exemplo, em uma transação bancária, o crédito e o débito – ambos – devem persistir na base de dados após a conclusão da operação.
25	O processo de consolidação de redescontos contratados e não liquidados gera redescontos em	O participante pode solicitar a consolidação de redescontos em aberto em uma única operação. Para isso, os redescontos existentes devem ser baixados para evitar

	duplicidade a pagar	duplicidade
26	O sistema fica vulnerável a ameaças devido a procedimentos de segurança inadequados, como a permanência de senhas *defaults* em hardware e software	As senhas originais que são utilizadas para instalar recursos de TI podem ser facilmente descobertas, gerando vulnerabilidade no ambiente
27	Ocorre contabilização incompleta de contratação ou liquidação de redesconto	Da mesma forma que a consistência de dados da uma operação de redesconto, os seus registros contábeis também devem ser íntegros ao final da transação
28	Ocorre entrada em produção de componente do sistema com defeito de software	A presença de defeito ou erro de software pode causar mau funcionamento do sistema e comprometer o processo de negócio
29	Ocorre entrada em produção de versões de componentes do sistema não homologados	Toda alteração nos componentes de software é homologada antes de ser instalada no ambiente de produção para garantir a qualidade e evitar riscos operacionais
30	Ocorre indisponibilidade total na Rede do Sistema Financeiro Nacional em seus dois *links*	A RSFN é o elo de ligação entre todos os participantes do SPB. Possui um *link* principal de telecomunicações e outro secundário para aumentar a disponibilidade da rede, por onde trafegam todas as mensagens
31	Ocorre o ingresso de participante não autorizado no sistema (cadastramento, certificado, habilitações internas, homologação)	O ingresso de um participante depende de seu cadastramento junto ao departamento competente, da criação de certificado de segurança, de habilitações internas no sistema e de sua passagem pelo ambiente de homologação
32	Ocorre problema no procedimento de uso ou atualização de certificados de segurança	Para trafegar na RSFN, a mensagem deve ser corretamente criptografada e assinada por meio de chaves públicas certificadas. Periodicamente, os participantes são obrigados a realizarem o procedimento de troca e divulgação de um novo certificado
33	Participante não habilitado ou não autorizado acessa o sistema de contingência de mensagens	Para entrar em regime de contingência de mensagens, o participante deve possuir operadores previamente cadastrados, que são devidamente autorizados a acessar o sítio do BC para contingência, quando solicitado
34	Um redesconto é gerado pelo sistema com o mesmo número identificador de um redesconto antigo	Cada operação de redesconto recebe um número identificador único no sistema, o qual serve de referência para futuras consultas, consolidações e liquidações
35	Uma contratação de redesconto, sem que haja lastro de títulos, é efetivada pelo sistema	As operações de redesconto devem seguir o modelo de entrega contra pagamento
36	Uma liquidação de redesconto é efetivada sem que haja reserva	Para liquidar um redesconto, o participante deve possuir reservas bancárias suficientes para receber seu título

	bancária suficiente	deixado como garantia
37	Uma mensagem de redesconto, originada por um não-participante do sistema, é processada	Somente os participantes detentores de conta de reservas bancárias e devidamente cadastrados no sistema podem solicitar redesconto
38	Uma mensagem não autorizada de redesconto é processada pelo sistema	As mensagens somente podem ser processadas durante a grade horária definida para cada mensagem
39	Uma resposta do processamento de redesconto é enviada indevidamente a outro participante	Após concluir o processamento, o sistema encaminha ao solicitante a resposta da contratação ou liquidação de redesconto, para que ele possa sensibilizar seus controles de fluxos de caixa

Fonte: Dados de pesquisa

Os 39 riscos operacionais identificados no processo de redesconto bancário, conforme os Quadros 19 e 20, serviram de base para a etapa seguinte da coleta de dados, na qual foram avaliadas as contribuições dos seis processos de governança de tecnologia da informação para a mitigação desses riscos.

4.2 Processos de Governança de Tecnologia da Informação

Para a avaliação dos processos de governança de tecnologia da informação na mitigação dos riscos operacionais foi adotada uma abordagem quantitativa, com uso de questionário eletrônico para a coleta de dados, com amostragem não-probabilística intencional ou por julgamento. Utilizou-se a estatística descritiva e análise de freqüências, com auxílio do pacote estatístico SPSS versão 13.0.

O questionário eletrônico, elaborado no banco de dados MS Access, foi encaminhado para especialistas da área de Tecnologia da Informação, os quais participaram do projeto de desenvolvimento do Sistema de Pagamentos Brasileiro. Ao todo, foram encaminhados 12 questionários para profissionais das áreas de desenvolvimento de sistemas, gerenciamento de banco de dados, segurança de sistemas, escritório de projetos, administração de dados e administração de redes. O índice de retorno foi de 67%, um total de 8 questionários respondidos.

Os seis processos de governança de tecnologia da informação avaliados nesta etapa foram aqueles apresentados no modelo conceitual da pesquisa: Avaliação e Gestão de Riscos, Gestão de Projetos, Continuidade de Serviços, Segurança de Sistemas, Gestão de RH e Gestão de Dados.

Para avaliar o grau de importância de cada um desses processos para a mitigação dos riscos operacionais identificados, foi elaborada uma escala intervalar do tipo Likert de 5 pontos, estruturada nas intensidades (1) Ínfima, (2) Baixa, (3) Moderada, (4) Alta e (5) Suprema. Foi acrescentada, ainda, a opção "Não Sei" para a situação correspondente. O informante poderia acessar a descrição resumida dos processos quando necessário.

Desta forma, para cada um 39 dos riscos operacionais, foram relacionados os 6 processos de tecnologia da informação e solicitado ao informante que avaliasse a contribuição de cada processo na mitigação do respectivo risco operacional, na escala de 1 a 5. Assim, os 6 processos foram avaliados com relação aos 39 riscos operacionais. Ao todo, cada processo de TI foi avaliado 312 vezes (39 riscos x 8 questionários respondidos).

A seguir, para cada um dos processos de TI, são apresentadas as freqüências das distribuições amostrais, o histograma com a curva normal e, em seguida, a análise dos dados.

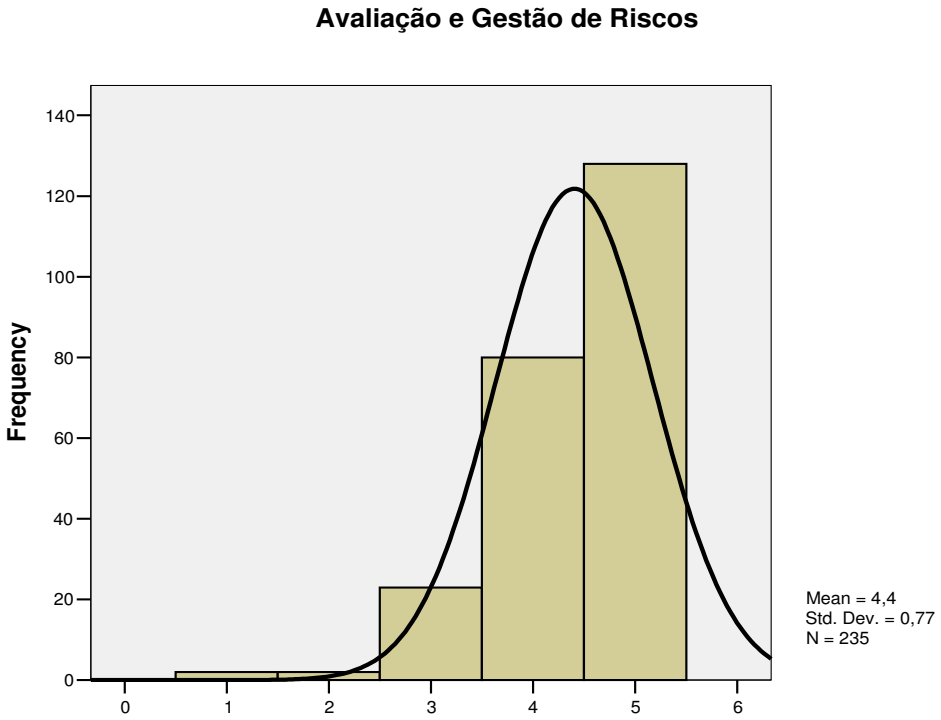
4.2.1 Avaliação e Gestão de Riscos

Tabela 1 – Avaliação e Gestão de Riscos – Distribuição de Freqüências

Contribuição do Processo	Freqüência		Freq. Acumulada
	n	%	%
Suprema	128	41,0	41,0
Alta	80	25,6	66,6
Moderada	23	7,4	74,0
Baixa	2	0,6	74,6
Ínfima	2	0,6	75,2
Não opinou	77	24,8	100
	312		

Fonte: Dados primários

Gráfico 1 – Avaliação e Gestão de Riscos – Histograma



A análise da Tabela 1 e do Gráfico 1 leva à constatação de que existe uma forte consideração do processo de Avaliação de Gestão de Riscos como tendo importância suprema na mitigação dos 39 riscos operacionais identificados, chegando a 41% da amostra. Em seguida, em outras 25,6% das respostas obtidas, foi considerada alta a sua contribuição, totalizando 66,6% nesses níveis mais altos da escala.

A média das respostas foi de 4,4 com desvio padrão de 0,77, o que sugere a grande importância deste processo de tecnologia da informação para a mitigação de riscos operacionais.

Do total de 312 avaliações realizadas na amostra, 77 delas não opinaram. Este número é repetido nos quadros a seguir.

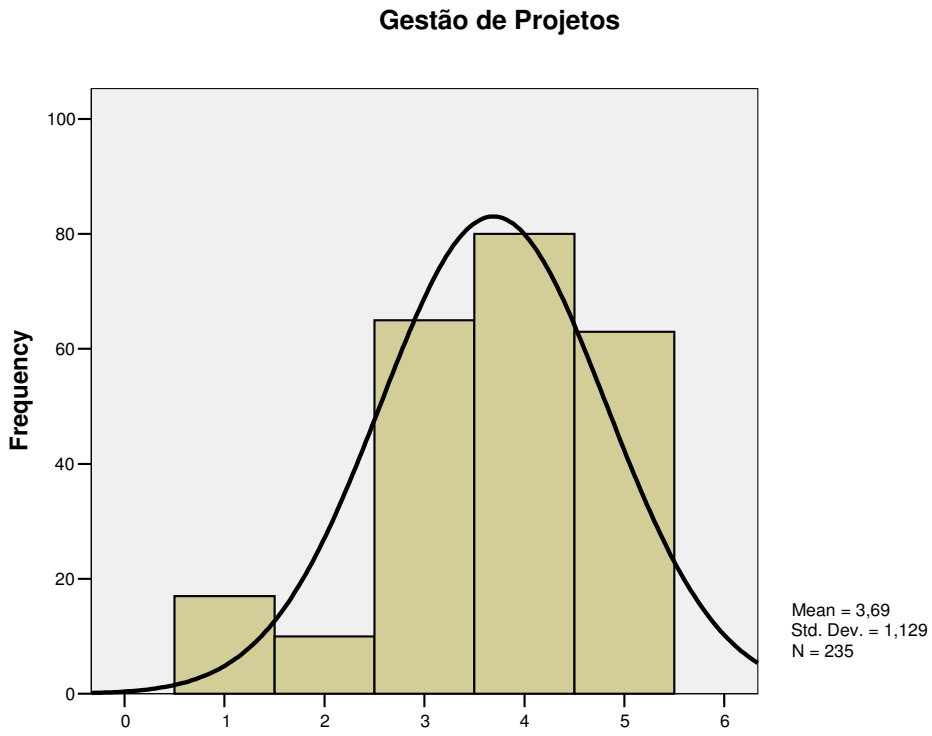
4.2.2 Gestão de Projetos

Tabela 2 – Gestão de Projetos – Distribuição de Freqüências

Contribuição do Processo	Freqüência		Freq. Acumulada
	n	%	%
Suprema	63	20,2	20,2
Alta	80	25,6	45,8
Moderada	65	20,8	66,6
Baixa	10	3,2	69,8
Ínfima	17	5,4	75,2
Não opinou	77	24,8	100
	312		

Fonte: Dados primários

Gráfico 2 – Gestão de Projetos – Histograma



A Tabela 2 e o Gráfico 2 sugerem que a avaliação do processo Gestão de Projetos na mitigação de riscos operacionais é mais uniformemente distribuída, com respostas mais proporcionais nas intensidades (3) moderada, 4(alta) e (5) suprema. Neste caso, um total de 66,6% das respostas foi obtido nesses 3 níveis de contribuição, sendo o grau "alto" a moda na distribuição, com 25,6%.

A média das respostas foi de 3,69 com desvio padrão de 1,129, o que sugere uma participação de moderada a alta do processo de Gestão de Projetos na mitigação dos riscos operacionais identificados no processo de negócio de redesconto bancário.

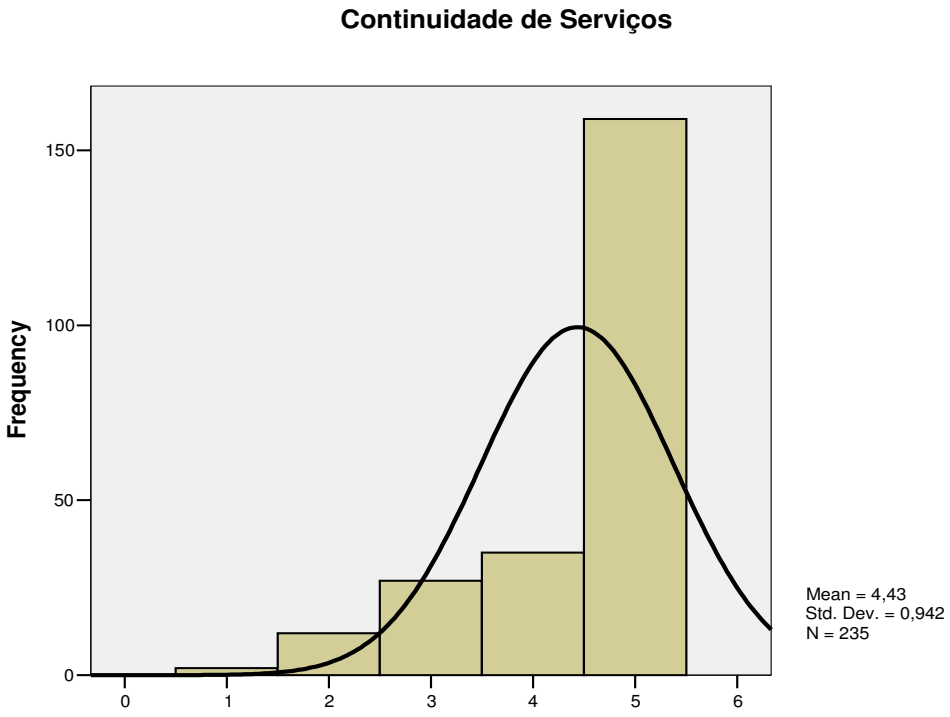
4.2.3 Continuidade de Serviços

Tabela 3 – Continuidade de Serviços – Distribuição de Freqüências

Contribuição do Processo	Freqüência		Freq. Acumulada
	n	%	%
Suprema	159	51	51
Alta	35	11,2	62,2
Moderada	27	8,7	70,9
Baixa	12	3,8	74,7
Ínfima	2	0,5	75,2
Não opinou	77	24,8	100
	312		

Fonte: Dados primários

Gráfico 3 – Continuidade de Serviços – Histograma



A partir da análise da Tabela 3 e do Gráfico 3, pode-se afirmar que é extremamente importante a contribuição do processo Continuidade de Serviços na mitigação dos riscos operacionais encontrados nesta pesquisa. O grau máximo de contribuição foi considerado em 51% das respostas, com grande destaque no histograma apresentado. Com exceção dos que não opinaram, somente 13% não consideraram esse processo como de alta ou suprema importância para a mitigação dos riscos.

A média das respostas foi de 4,43 com desvio padrão de 0,942, o que sugere a grande importância deste processo de tecnologia da informação para a mitigação de riscos operacionais.

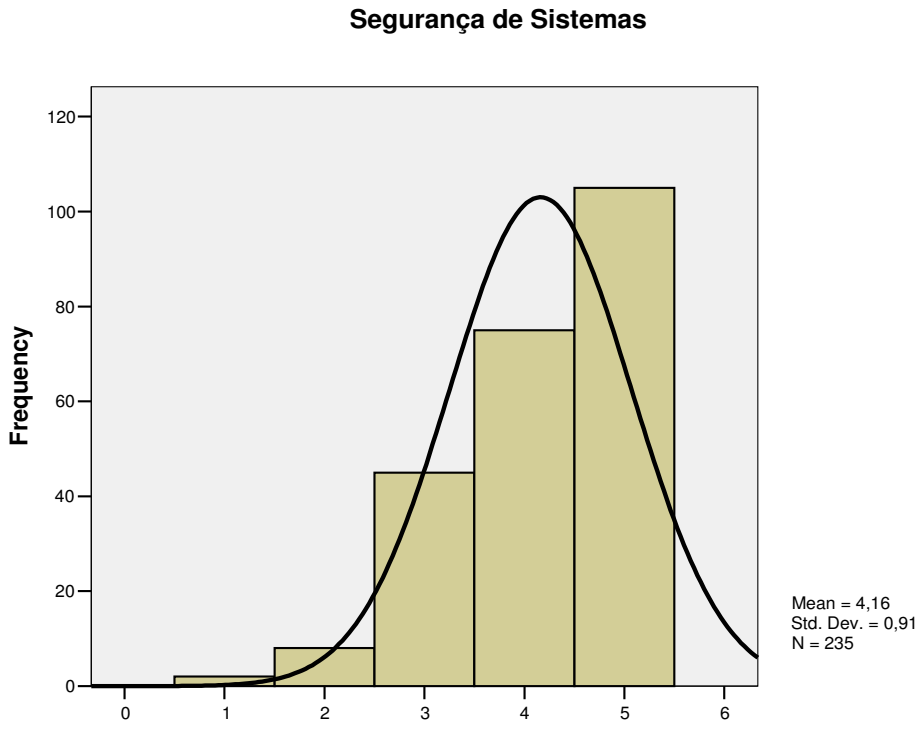
4.2.4 Segurança de Sistemas

Tabela 4 – Segurança de Sistemas – Distribuição de Freqüências

Contribuição do Processo	Freqüência		Freq. Acumulada
	n	%	%
Suprema	105	33,7	33,7
Alta	75	24	57,7
Moderada	45	14,4	72,1
Baixa	8	2,6	74,7
Ínfima	2	0,5	75,2
Não opinou	77	24,8	100
	312		

Fonte: Dados primários

Gráfico 4 – Segurança de Sistemas – Histograma



A Tabela 4 e o Gráfico 4 revelam, para o processo de Segurança de Sistemas, uma participação moderada de aproximadamente 14% na mitigação dos 39 riscos operacionais avaliados, com acréscimo de 10% para o nível "alto", que totalizou 24%, e acréscimo de outros 10% para o nível extremo superior da escala, que totalizou aproximadamente 34% das respostas. Juntos, esses 3 níveis acumularam 72,1% das avaliações realizadas. O histograma evidencia esta evolução comparativa entre os níveis 3, 4 e 5 da escala utilizada.

A média das respostas foi de 4,16 com desvio padrão de 0,91, sugerindo que a contribuição do processo de tecnologia da informação denominado Segurança de Sistemas tende ao grau "alto" para a mitigação dos riscos operacionais identificados no processo de negócio de redesconto bancário.

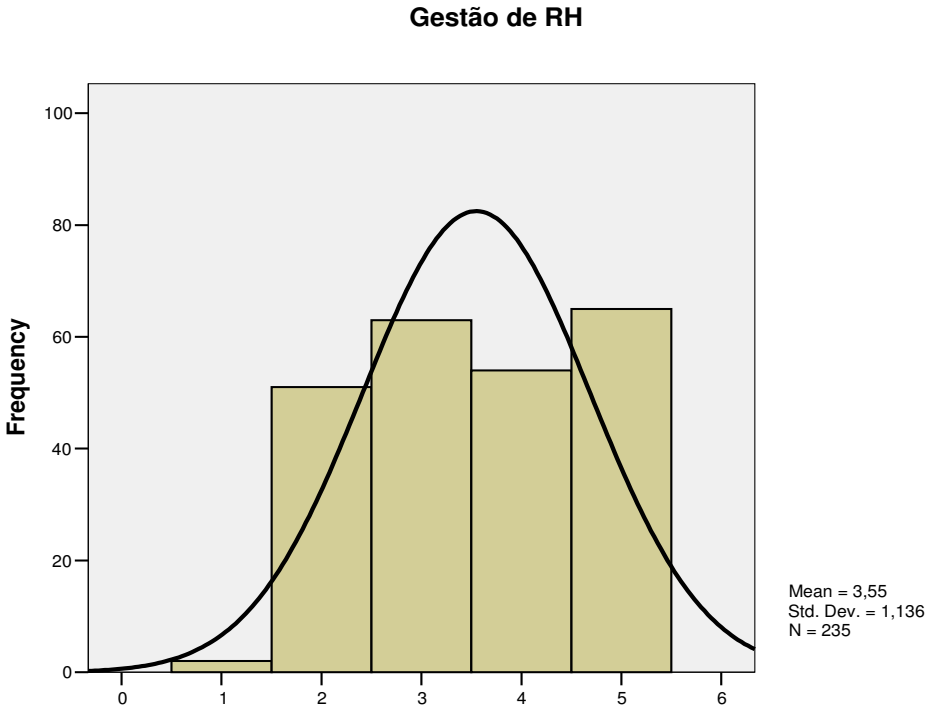
4.2.5 Gestão de RH de TI

Tabela 5 – Gestão de RH de TI – Distribuição de Freqüências

Contribuição do Processo	Freqüência		Freq. Acumulada
	n	%	%
Suprema	65	20,8	20,8
Alta	54	17,3	38,1
Moderada	63	20,2	58,3
Baixa	51	16,3	74,6
Ínfima	2	0,6	75,2
Não opinou	77	24,8	100
	312		

Fonte: Dados primários

Gráfico 5 – Gestão de RH de TI – Histograma



O processo de Gestão de RH de TI referente à área de tecnologia da informação foi o que apresentou melhor simetria na distribuição das respostas, conforme se observa na Tabela 5 e no Gráfico 5. Com exceção da avaliação extrema inferior da escala, todas as outras apresentaram concentração de respostas entre 16 e 21%. Em relação aos outros processos de TI avaliados, o processo de Gestão de RH apresentou a maior freqüência de respostas no grau "baixo", com 16,3% das avaliações.

A média das respostas foi de 3,55 com desvio padrão de 1,136, o que sugere uma participação de baixa a moderada do processo de Gestão de RH na mitigação dos riscos operacionais identificados.

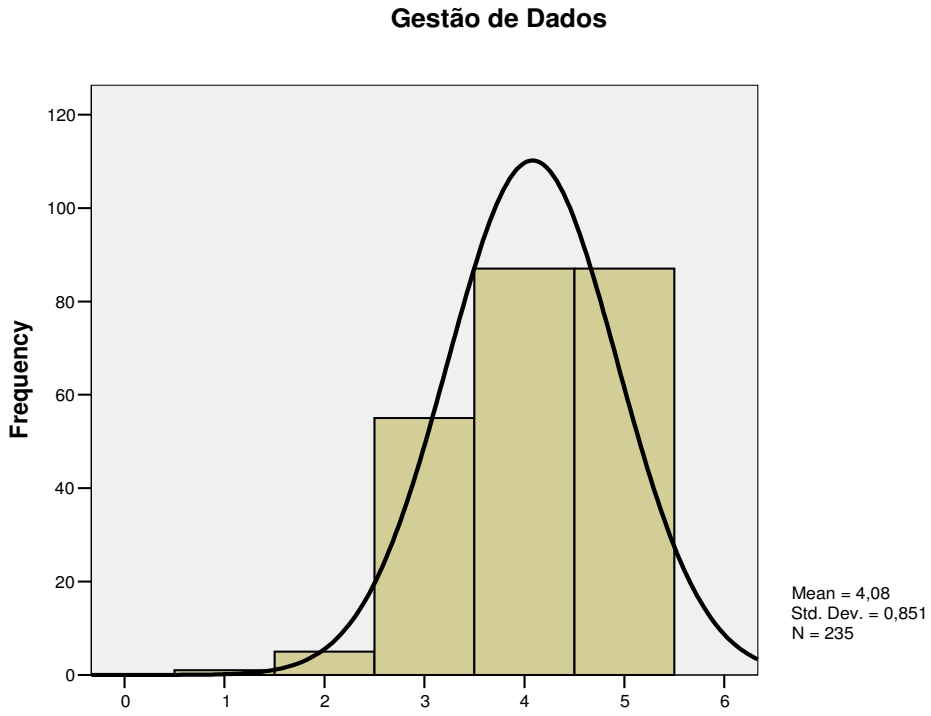
4.2.6 Gestão de Dados

Tabela 6 – Gestão de Dados – Distribuição de Freqüências

Contribuição do Processo	Freqüência		Freq. Acumulada
	n	%	%
Suprema	87	27,9	27,9
Alta	87	27,9	55,8
Moderada	55	17,6	73,4
Baixa	5	1,6	75
Ínfima	1	0,2	75,2
Não opinou	77	24,8	100
	312		

Fonte: Dados primários

Gráfico 6 – Gestão de Dados – Histograma



Finalmente, a análise da Tabela 6 e do Gráfico 6 revela a existência de 2 modas na distribuição de freqüências para o processo de Gestão de Dados. Somados, esses dois itens superiores da escala, totalizam 55,8% das respostas. Em seguida, com 17,6%, aparece o grau "moderado" de contribuição para a mitigação dos riscos operacionais, totalizando 73,4% nesses 3 níveis da escala.

A média das respostas foi de 4,08 com desvio padrão de 0,851, o que sugere uma participação com tendência ao grau "alto" do processo de Gestão de Dados na mitigação dos riscos operacionais identificados.

4.2.7 Estatística Descritiva dos Processos

A Tabela 7 apresenta a estatística descritiva da amostra, em ordem decrescente da média da importância de cada processo analisado anteriormente.

Tabela 7 – Estatística Descritiva da Amostra de Processos de TI

Processos	Média	Desvio Padrão	Moda (Grau)	Assimetria	Curtose
1-Continuidade de Serviço	4,43	0,94	Suprema	- 1,59	1,59
2-Avaliação e Gestão de Riscos	4,40	0,77	Suprema	- 1,41	2,50
3-Segurança de Sistemas	4,16	0,91	Suprema	- 0,88	0,21
4-Gestão de Dados	4,08	0,85	Suprema/Alta	- 0,53	- 0,36
5-Gestão de Projetos	3,69	1,13	Alta	- 0,77	0,12
6-Gestão de RH de TI	3,55	1,14	Suprema	- 0,09	- 1,27

Fonte: Dados primários
* Não foram consideradas no cômputo das médias as respostas dos que não opinaram

A medida de assimetria (*skewness*) indica a distribuição da amostra em relação à curva normal. O valor zero indica a simetria perfeita. Números negativos de assimetria indicam a concentração das respostas em valores altos, à direita da média, enquanto que indicadores positivos apontam para a concentração das respostas em valores baixos.

A medida de curtose (*kurtosis*) é um indicador de elevação ou do achatamento de uma distribuição quando comparada com uma distribuição normal. O valor zero indica a distribuição normal. Valores positivos indicam uma distribuição relativamente elevada e valores negativos, uma distribuição relativamente achatada.

Na Tabela 7, as médias dos 4 primeiros processos indicam que o seu grau de contribuição na mitigação dos riscos operacionais está entre alto e supremo, respectivamente 4 e 5 na escala utilizada. Os dois últimos processos foram considerados de importância moderada a alta, com um desvio-padrão maior que os demais, demonstrando maior dispersão das respostas em torno da média.

Percebe-se que a medida de assimetria está fortemente correlacionada com a média. O índice de correlação entre assimetria e média foi calculado em -0,87, próximo de -1, que seria uma correlação perfeita. O sinal negativo indica a correlação inversamente proporcional. Nos processos de 1 a 6, enquanto a média diminui, aproximando-se do ponto médio da escala, o valor da assimetria aumenta, indicando uma maior simetria na distribuição, chegando próximo à simetria perfeita no último processo (-0,09).

A localização da moda das distribuições no grau máximo da escala em quase todos os casos, certamente deslocou a média para o lado direito da distribuição. Os valores de curtose indicam a formação de curvas de distribuição com formato elevado nos 2 primeiros processos, formato mais próximos à curva normal nos 3 processos seguintes, e, finalmente, uma curva com formato mais achatado no último processo. O coeficiente de correlação entre a média e a curtose foi de 0,84, indicando que a média diminui correlacionada com a diminuição da curtose.

Realizou-se o teste não-paramétrico U de *Mann Whitney* para verificar se há diferença estatisticamente significativa, ao nível de confiança de 95%, entre as médias de importância dos processos de TI para mitigação de riscos operacionais nos dois grupos: (I) Rotina Diária; e (II) Circunstanciais (Quadros 19 e 20). Com isso, pode-se verificar se os processos de TI atuam de maneira diferente nos dois tipos de riscos. A Tabela 8 traz o cálculo separado das médias para ambos os grupos. A Tabela 9 exibe o cálculo do referido teste não-paramétrico.

Tabela 8 – Cálculo das Médias de Importância dos Processos de TI, por Tipo de Risco

Tipo de Risco	Gestão e Avaliação de Riscos	Gestão de Projetos	Continuidade de Serviços	Segurança de Sistemas	Gestão de RH	Gestão de Dados
Rotina Diária	4,27	3,42	4,51	3,90	3,43	4,05
Circunstanciais	4,49	3,87	4,39	4,33	3,63	4,10
Total	4,40	3,69	4,43	4,16	3,55	4,08

Fonte: SPSS, com base nos dados primários

Tabela 9 – Teste não-paramétrico U de Mann Whitney

Test Statistics [a]

	Gestão e Avaliação de Riscos	Gestão de Projetos	Continuidade de Serviços	Segurança de Sistemas	Gestão de RH	Gestão de Dados
Mann-Whitney U	5772,500	5098,500	6129,500	4885,500	5995,500	6359,000
Wilcoxon W	10143,500	9469,500	16282,500	9256,500	10366,500	10730,000
Z	-1,824	-3,078	-1,122	-3,611	-1,231	-,509
Asymp. Sig. (2-tailed)	,068	**,002**	,262	**,000**	,218	,611

[a] Grouping Variable: Tipo de Risco

Fonte: SPSS, com base nos dados primários

A hipótese nula é de que não há diferença estatisticamente significativa entre as médias dos dois grupos. Considerando o nível de significância $\alpha = 0,05$, que indica uma confiança de 95% de rejeitar corretamente a hipótese nula, verifica-se (Tabela 9), que, nos casos dos processos Gestão de Projetos ($p = 0,002$) e Segurança de Sistemas ($p = 0$) existe diferença significativa, ao nível de significância estabelecido, entre as médias dos grupos comparados, pois $p < \alpha$ nos dois casos.

A rejeição destas duas hipóteses nulas leva a crer que a importância desses dois processos de TI para a mitigação dos riscos operacionais é significativamente diferente em cada grupo. Na Tabela 8, observa-se que a média desses dois processos é maior para os riscos do tipo II (hipotéticos ou circunstanciais). Ou seja, os processos de Gestão de Projetos e Segurança de Sistemas têm maior impacto na mitigação dos riscos operacionais identificados ao nível hipotético do que aqueles da rotina diária.

Diante das evidências apresentadas nas análises individuais dos processos de tecnologia da informação, constantes nos itens 4.2.1 a 4.2.6, e também da análise realizada com base na Tabela 7, é razoável considerar que todos os processos avaliados são importantes fontes de contribuição para a mitigação dos riscos operacionais identificados na pesquisa, na ordem de relevância adotada em função dos indicadores da mesma tabela.

Desta forma, os processos de governança de TI denominados Continuidade de Serviços, Avaliação e Gestão de Riscos, Segurança de Sistemas, Gestão de Dados, Gestão de Projetos e Gestão de Recursos Humanos de TI, nesta ordem, foram considerados como elementos relacionados à mitigação de riscos operacionais levantados no processo de redesconto bancário.

A seguir, é investigada a importância dos processos de controle de governança de tecnologia da informação.

4.3 Processos de Controle Governança de Tecnologia da Informação

No decorrer do estudo de caso, percebeu-se a necessidade de realizar uma coleta de dados à parte para a avaliação dos dois processos de controle de governança de TI, os quais não estão diretamente relacionados à operacionalização do processo de redesconto bancário, mas à governança corporativa e à auditoria interna. Desta forma, a análise a seguir não enfoca o processo de redesconto bancário em si, mas a importância dos dois processos de controle para a mitigação de riscos operacionais de uma maneira geral.

Os dois processos analisados neste item foram Promoção de Governança de TI e Avaliação e Monitoramento de Controles Internos. Eles pertencem ao domínio chamado

Monitoramento e Avaliação do modelo adotado como referência para o estudo, e possuem seu foco em aspectos de monitoramento e controle interno. Foram avaliados por respondentes de uma área especifica da organização, o Departamento de Auditoria Interna (DEAUD).

Nesta etapa do levantamento, foram realizadas três entrevistas, duas seguindo o protocolo do Anexo D, e a outra com auxílio do questionário eletrônico (Anexo F). A seguir, utiliza-se a análise de conteúdo para o tratamento dos dados.

4.3.1 Promoção de Governança de TI

Após realizar pesquisas, observação de mercado e participação em eventos, o Departamento de Auditoria Interna adotou o *framework* COBIT como referência em suas recomendações para tratar de assuntos da área de tecnologia da informação e auxiliar nas atividades de auditoria com foco em risco: "A nossa metodologia não estava adequada com relação às boas práticas (de governança de TI) (O COBIT) é a espinha dorsal. Daí nós partimos para outros modelos, específicos para cada tipo de processo, para chegar a um detalhamento maior. O nível de detalhamento do Cobit é um pouco elevado" (Resp 13).

A adoção de um modelo de referência traz algumas vantagens para a organização: "Quando a gente adota um modelo, a coisa fica impessoal (...) Não vai depender tanto da experiência do auditor (...) O auditor chega com uma visão mais ampla (...) A gente está referenciado em boas práticas. Então alguns riscos que não são observados pelo gestor a gente tem essa visão, antes" (Resp 13).

Outros órgãos do governo também adotaram o mesmo modelo de referência em seus trabalhos de auditoria com foco em risco de TI: "Todo o sistema de controle da União, tanto a CGU (Controladoria Geral da União) quanto o TCU (Tribunal de Contas da União) estão baseados no Cobit para fazer auditoria". Assim, os processos de governança de TI tendem a serem institucionalizados: "Pode vir com um poder de determinação" (Resp 13).

Nesse sentido, as áreas de auditoria interna e externa estão liderando a promoção da governança de TI, uma vez que a conscientização e a comunicação são aspectos iniciais no modelo de maturidade de processos, conforme aponta o ITGI (2007b). Desta forma, buscam

contribuir também para o alcance do terceiro elemento da Figura 3 (p. 32), a governança: “Na minha percepção, estamos na fase de conscientização” (Resp 14).

Ainda, na análise da promoção da governança corporativa e, por conseguinte, da governança de tecnologia da informação, outros atributos são essenciais. O estabelecimento de estruturas organizacionais, papéis e lideranças para o alcance dos objetivos de TI em linha com os objetivos estratégicos são denotados no processo de Promoção e Governança de TI, assim como em OCDE (2004) e BIS (2006), que colocam, ainda, a importância do monitoramento e dos incentivos adequados para o alcance dos interesses da empresa e de seus acionistas. Meirelles *et al.* (2005) incluem a transparência e a responsabilização, esta última também citada por Pinochet *et al.* (2005).

Segundo os entrevistados, o fomento à discussão organizacional do planejamento estratégico de TI tende a incrementar a transparência e contribuir para o alinhamento tático-estratégico da tecnologia da informação. Esta tendência de esforços conjuntos entre executivos de negócio e executivos de TI é observada por Albertin e Albertin (2005).

Por sua vez, a criação de uma estrutura organizacional, a responsabilização e o estabelecimento de papéis para a governança corporativa é fundamental para a evolução interna da governança de TI: “Para mim, a quem compete fazer a governança é a grande questão (...) A instituição tem a sua responsabilidade também. Não é só do pessoal” (Resp 14). Há um grupo de trabalho que vem realizando estudos para a definição de um modelo de governança corporativa para a instituição, bem como para o estabelecimento de políticas, procedimentos, ferramentas e integração da gestão de riscos. “Aí talvez a governança de TI dê um salto de qualidade muito grande” (Resp 14).

A importância dos incentivos adequados para a governança também foi destacada: “Se você não dá o suporte que essa equipe precisa, não vai conseguir emplacar de jeito nenhum! (...) Tem que vir o instrumento de delegação de competência, baixar normas, descrever o processo, dar os recursos necessários” (Resp 13). “O patrocínio da alta direção tem que ser muito forte. Comprometimento mesmo. Patrocínio não é só chegar e dizer que apóia. Tem que estar confirmando em todas as oportunidades. Dar autoridade para quem precisa” (Resp 14).

No entanto, a principal barreira identificada para implementação da governança de TI está na esfera de poder, na especificação dos direitos decisórios, elemento de governança descrito por Weill e Ross (2006): “Existe uma série de fatores pessoais, funcionais, culturais que impacta a implementação (...) Tem perda de poder envolvido nesse modelo de governança, onde o chefe de TI vai perder poder sim, apesar de ter uma série de vantagens” (Resp 13). “A implantação é difícil porque você mexe com o poder das pessoas” (Resp 14).

Houve unanimidade entre os respondentes na afirmativa da importância do processo de promoção de governança de TI, sendo referenciado como a base para a implantação ou evolução dos demais processos do modelo COBIT, como aqueles analisados no item 4.2, os quais mostraram-se importantes para a mitigação de riscos operacionais.

Os princípios do Novo Acordo de Basiléia (Quadro 3, p. 38) guardam relacionamentos com a governança de TI. A atuação da alta administração para o patrocínio na implementação, particularmente do 1º e do 2º princípios do Basiléia II, passa pelo processo Promoção e Governança de TI, no que tange à busca de alinhamento estratégico entre as áreas de negócio e de tecnologia da informação, entrega de valor e gestão de riscos operacionais de TI.

Desta forma, o processo Promoção de Governança de TI atua, mesmo que indiretamente, como suporte fundamental na mitigação de riscos operacionais, tendo papel estratégico, no modelo de boas práticas, para a eficácia da governança.

4.3.2 Avaliação e Monitoramento de Controles Internos

Da mesma forma que a análise do processo anterior, buscou-se compreender a contribuição do processo de Avaliação e Monitoramento de Controles Internos sem a relação direta com o processo de redesconto bancário, mas com a gestão de riscos operacionais de uma forma geral.

Observou-se que o trabalho de auditoria interna na organização vem, gradativamente, alterando seu foco de trabalho para o controle interno com foco em risco, tendência comentada por Bergamini Jr (2005). Ou seja, além da função de *compliance* para verificar o atendimento a regulamentações, busca-se a gestão de riscos em suas atividades, conforme

indicado na Figura 3 (p. 32), que ilustra a estrutura integrada de gestão de riscos sugerida pelo COSO.

Este mudança de foco nos controles internos para a gestão de riscos tem motivado a melhoria do sistema de controles internos na organização – ambiente de controle, avaliação de riscos, atividades de controle, informação e comunicação e atividades de monitoramento – COSO (1994) e BIS (1998), especialmente nas atividades ligadas à tecnologia da informação: "A gente está levando...tentando levar a organização a ter essa visão, principalmente o DEINF (Departamento de TI), de que é preciso sempre buscar melhorar seus processos e adequar ao modelo de governança mas aceito no mercado. Essa é a visão não só do DEAUD, mas de todo o sistema de controle da União" (Resp 13). Os elementos do sistema de controles internos são a seguir analisados.

O ambiente de controle vem se desenvolvendo, uma vez que os valores e competências essenciais à gestão de riscos têm sido promovidos por iniciativas como a do DEAUD e também do DEINF, que recebeu do IT Service Management Fórum (itSMF), em 2007, o prêmio "Projeto do ano" que objetiva implantar melhores práticas de gestão de TI descritas pelo *framework* ITIL para governança de TI. O projeto, que está em desenvolvimento há três anos, foi eleito por representantes da comunidade de TI de todo o Brasil. Já foram implementados quatro processos operacionais: gestão de incidentes, de problemas, de mudanças e de configuração.

A avaliação de riscos vem sendo apoiada pelo processo de Avaliação e Monitoramento de Controles Internos, uma vez que a identificação e análise de riscos operacionais são realizadas por funções de controle internas e externas: "A visão deles (externa) é um pouco mais ampla que a nossa. A gente entra em um detalhe maior (...) A gente ajuda a ir nessa direção (...) recomendamos (à área de TI) os processos, ajustes de controle" (Resp13).

As atividades de controle, outro elemento do sistema de controles internos, são também apoiadas pelo processo de Avaliação e Monitoramento de Controles Internos: "Os objetivos de controle que o *framework* fornece é exatamente o controle para mitigar o risco" (Resp 14). "A gestão de riscos, você faz em que nível? Você pode fazer no nível do objetivo de controle. Ou seja, os riscos que aquele objetivo de controle está tentando mitigar" (Resp 13). "Se você pega um objetivo de controle, a gente aqui está desmembrando isso em

elementos de controle. Porque um objetivo de controle pode mitigar um ou vários riscos. Para entrar no nível de avaliar os controles internos, a gente teve que quebrar em elementos de controle." (Resp 13).

O elemento de informação e comunicação para controles internos corresponde à existência de uma via dupla de informação entre os níveis organizacionais. Incentivado por meio da promoção de governança de TI, essa via de comunicação, inicialmente unidirecional, é incentivada a ser ecoada na organização. "Em toda a comunicação com o DEINF, a referência é o Cobit. Em termos práticos, você busca os riscos daquele processo de TI que existe dentro do DEINF. O Cobit te dá essa referência" (Resp 14). "De tanto o DEAUD falar, eles estão tendo uma visão de futuro. Está no PDTI (Plano Diretor de TI). (...) Sai uma recomendação de auditoria sempre baseada no Cobit. Eles vão ver: 'como é que eu resolvo isso?' Onde vai ter isso? No Cobit! (...) Vai ficar mais fácil. Fica melhor o diálogo e a nossa análise vai focar especificamente naquilo que foi estabelecido, no que está funcionando e no que não está" (Resp 13).

Por último, as atividades de monitoramento de controles internos foram percebidas como importantes para possibilitar o *feedback* na gestão de riscos: "Você faz o planejamento, você faz a aquisição, você entrega aquele serviço (...) Se você não monitora isso, como você vai saber se os controles que foram definidos estão trazendo os resultados necessários ou se precisa de algum ajuste?" (Resp 13).

A análise dos elementos do sistema de controles internos permite colocar o processo Monitoramento e Avaliação de Controles Internos como um típico processo de controle, como definido por Tannenbaum (1975), um ciclo em que a tentativa de influência é dirigida de A para B.

Pôde-se constatar, também, a validade da construção teórica apresentada por NIST (2002), representada na Figura 7 (p. 44), que trata da importância de controles para a mitigação de riscos. A atuação do controle é mais efetiva nas vulnerabilidades, enquanto que o controle das ameaças, muitas vezes externas, pode ser questionada: "Toda ameaça você pode até ter um controle, atacando a ameaça diretamente. Tem um hacker, você vai lá e prende (...) Você não controla a ameaça, você a elimina" (Resp 13).

Em resumo, a análise dos dois processos de controle acima, embora desvinculada do processo de redesconto, indica a existência de um relacionamento fundamental entre eles e a mitigação de riscos operacionais. A eficiência operacional é um objetivo dos controles internos. Avaliar e monitorar controles internos, com foco no risco, conduz à formação de um ambiente de controle em que a gestão de riscos é a base para essa eficiência.

A promoção da governança de TI leva ao desenvolvimento de uma estrutura adequada, com lideranças, recursos, incentivos, responsabilidades e decisões para permitir o alinhamento estratégico da TI às necessidades dos processos de negócio. A evolução dos processos de TI, como os seis analisados neste estudo, está fundamentada na boa Promoção de Governança de TI, isto é, na evolução das capacitações para essa promoção, que acaba por influenciar a maturidade de todos os processos de TI, como será visto a seguir.

4.4 Maturidade de Processos e Aplicabilidade para Gestão

A análise da maturidade dos processos de governança de TI selecionados para o estudo e a investigação da aplicabilidade da gestão de processos por meio desse indicador foram realizadas com base nos dados coletados a partir das entrevistas focadas nº 13 e 14 do Quadro 15 (p. 87) e da amostra intencional detalhada no Quadro 16 (p. 88). Com base no questionário do Anexo F, foi criado um novo questionário eletrônico para avaliação específica de maturidade dos dois processos de controle, para aplicação junto ao departamento de auditoria. No entanto, não houve êxito na aplicação deste questionário em virtude do esgotamento do tempo destinado às sucessivas etapas de coleta de dados. Obteve-se uma resposta do referido questionário .

Para obtenção dos indicadores de maturidade dos processos de governança de TI, foi confeccionado um simulador com base nos modelos de maturidade (Anexo A) de cada um dos processos selecionados. Para cada um dos 5 níveis de maturidade (Inicial, Repetido, Definido, Gerenciado e Otimizado), foram elaboradas 4 assertivas que refletiam suas características de consciência, comunicação, procedimentos, ferramentas, treinamento, responsabilização ou medidas de desempenho. Desta forma, cada respondente avaliou 20 assertivas de cada processo de TI (p. 177), totalizando 120 assertivas para a avaliação dos 6 processos.

Ao término dessa avaliação, o simulador apresentava o indicador aproximado das maturidades (p. 178), calculados em função das respostas fornecidas. Como exemplo, se fossem marcadas 2 assertivas do nível 1, 2 do nível 2, 1 do nível 3 e 4 do nível 4 para um processo, calculava-se o indicador de maturidade como a média (2x1 + 2x2 + 1x3 + 4x4) / 9 = 2,78. Em seguida, buscava-se, com perguntas abertas, a opinião do respondente com relação à aplicabilidade de modelos de maturidade, isto é, a coerência do indicador com a realidade organizacional bem como a sua utilidade para a gestão.

A Tabela 10 apresenta a estatística descritiva da amostra obtida na simulação de maturidade. É importante frisar que a análise dos respondentes se deu a partir de uma simplificação dos modelos de maturidade da estrutura COBIT. A obtenção mais acurada das reais maturidades demandaria recursos humanos e de tempo fora do alcance das possibilidades deste estudo.

Tabela 10 – Estatística Descritiva de Maturidade de Processos de TI

Processos	Maturidade	Nível mais próximo	Desvio Padrão
1-Gestão de Dados	3,38	3-Definido	1,05
2-Segurança de Sistemas	3,30	3-Definido	0,90
3-Gestão de Projetos	3,26	3-Definido	0,87
4-Continuidade de Serviços	2,89	3-Definido	0,89
5-Gestão de RH de TI	2,41	2-Repetido	0,99
6-Avaliação e Gestão de Riscos	2,37	2-Repetido	0,75
Média geral	2,93	3-Definido	0,45

Fonte: Dados primários

A média geral obtida (2,93) indica a tendência para o nível “definido” de maturidade, que se caracteriza pela existência de procedimentos padronizados e documentados – típicos de organizações burocráticas – os quais são comunicados e treinados, mas os desvios individuais provavelmente não são detectados.

As médias indicadas na Tabela 10 são próximas daquelas encontradas na *survey* de Guldentops *et al.* (2002), que indicou média entre 2,5 e 3 para empresas do setor financeiro, ou seja, processos com níveis de maturidade com tendência ao nível "definido".

A correlação entre as contribuições dos processos de TI para a mitigação de riscos (Tabela 7, p. 117) e os respectivos índices de maturidade é praticamente nula (ρ= -0,02), indicando que processos que mais contribuem para a mitigação de riscos operacionais não necessariamente possuem as maiores maturidades.

Considerado como o segundo processo mais importante para a mitigação de riscos operacionais, o processo "Avaliação e Gestão de Riscos" foi avaliado com o menor indicador de maturidade entre os processos. Isso sugere que a maior maturidade dos demais processos de governança de TI pode compensar uma relativa deficiência desse processo, o qual está fortemente relacionado à gestão de riscos operacionais.

A evolução das capacitações no conjunto de processos de TI está diretamente ligada à maior maturidade para mitigar riscos. Além das tecnologias de conhecimento necessárias para o desenvolvimento dos processos de TI em si, a evolução da maturidade do processo depende de atributos como consciência e comunicação; políticas, planos e procedimentos; ferramentas e automação; habilidades e competência; responsabilidade e prestação de contas; e estabelecimento de objetivos e medidas de desempenho.

Tais atributos foram validados e parecem refletir o caminho progressivo em direção ao último nível de maturidade: "Você começa a trabalhar as pessoas. Você vê o processo: (0) ninguém tem consciência; (1) alguém tem consciência; (2) uma equipe já consegue executar aquilo ali de uma forma igual (...) A maturidade vem evoluindo nas pessoas e chega depois na organização" (Resp 13).

A passagem do nível 2 para o nível 3 de maturidade requer uma mudança de paradigma na gestão dos processos. Até o nível 2 (repetido), pode-se dizer que o processo está no plano individual, com consciência incipiente. Existem pessoas-chave que dominam o processo. Para atingir o nível 3, o processo deve passar para o plano institucional, pertencendo à organização, não mais ao indivíduo. Isto implica em mudança cultural, o que por vezes cria barreiras para governança de TI: "A partir do momento que você vem com um modelo de

governança que quebra todo esse paradigma, fica bem mais difícil de implementar isso" (Resp 13). "As pessoas-chave não ganham nada com a evolução na maturidade" (Resp 14).

A evolução da maturidade dos processos de TI para a mitigação de riscos operacionais depende, portanto, diretamente da maturidade de processos de controle do modelo. A promoção da governança de TI, visando ao estabelecimento da estrutura, dos papéis, das responsabilidades e das lideranças organizacionais para a governança de TI, influencia os processos institucionais, dentro do conceito de governança corporativa de Turnbull (1997). Confere-lhes o patrocínio necessário para a conscientização, comunicação e elaboração de planos, políticas e procedimentos necessários. E a consolidação de um sistema de controles internos, com foco na gestão de riscos, passa pela avaliação e monitoramento de controles dos processos de tecnologia da informação para que os processos de negócio atinjam seus objetivos, com eficiência operacional.

Com relação aos dos indicadores de maturidade, também foram investigadas a coerência com a realidade organizacional dos valores encontrados na simulação individual e a aplicabilidade dos indicadores para a gestão de processos. De um total de 7 questionários que avaliaram esses itens, 2 respondentes concordaram com os valores obtidos pela simplificação do modelo de maturidade.

Outros 4 respondentes concordaram parcialmente: "Acredito que o item 'Avaliação e Gestão de Riscos de TI' ficou abaixo do esperado com a realidade da Instituição: imagino que estamos no nível 4, Gerenciado" (Quest 3); "A Gestão de RH é responsabilidade de outro departamento (...) Muitas perguntas foram do tipo 'está sendo feito?' e permitem duas situações distintas para sua negativa: Não está sendo feito porque já foi feito e concluído; Não está sendo feito porque nem se começou a fazer" (Quest 6); "Possivelmente questões relativas a Segurança de Sistemas de TI tenham sido sub-avaliadas, creio que a organização se encontra neste ponto em um nível mais alto" (Quest 10); "Ela não captura o movimento, melhora ou piora, do controles" (Quest 11).

Um dos respondentes não concordou com os indicadores obtidos: "O conjunto de assertivas formuladas não é suficiente para avaliar consistentemente o nível de maturidade de processos da organização. A proposição de respostas binárias dificulta a avaliação e há várias

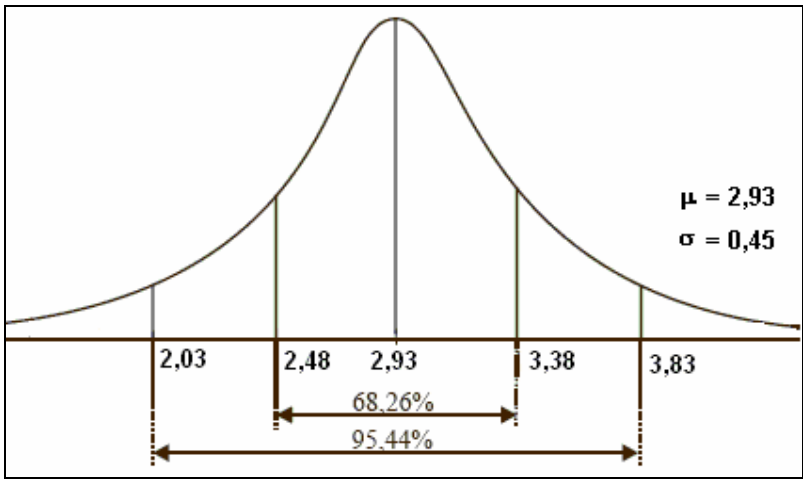
assertivas compostas, o que exige uma avaliação que pode não corresponder à realidade de parte da assertiva" (Quest 2).

De uma forma geral, a simulação de modelos atingiu o seu objetivo, que era criar um contexto de avaliação de maturidade, embora sem um diagnóstico preciso dos indicadores. Vale reafirmar que os valores encontrados são aproximações obtidas pela simplificação dos modelos de maturidades, e que, para a maioria dos respondentes, foi considerada parcialmente coerente com a situação organizacional.

Aliás, o diagnóstico da maturidade de um processo mostrou-se útil para a sua gestão, corroborando Santos (2003), conforme opiniões nesse sentido: "É um instrumento de referência para fazer um *gap* análise (...) Para medir em que nível que estou e pra onde quero ir" (Resp 13); "A premissa é a de que só conseguimos gerenciar aquilo que realmente conseguimos medir" (Quest 1).

Entretanto, a gestão de processos por maturidade parece estar vinculada a processos com maturidade de nível 4 (gerenciado), que se caracteriza pelo monitoramento e medição para o contínuo aperfeiçoamento. A *survey* de Guldentops *et al.* (2002) encontrou média de maturidade igual a 3, próximo da média encontrada nesta pesquisa. Para efeito ilustrativo, considerando a média e o desvio-padrão amostrais da Tabela 10 como os verdadeiros parâmetros da população de processos de TI com distribuição normal, observa-se, no Gráfico 7, que cerca de 95% das maturidades estariam entre 2,03 e 3,83, a dois desvios-padrão da média, e aproximadamente 2% dos processos teriam nível de maturidade maior ou igual a 4.

Gráfico 7 – Distribuição Normal de Maturidade



Assim, de uma maneira geral, a gestão contínua de processos por maturidade, apesar de sua utilidade, parece ser ainda um desafio no que se refere ao seu uso nos processos de governança de tecnologia da informação.

Diante das análises realizadas com relação à contribuição dos processos de tecnologia da informação e dos processos de controle para a mitigação de riscos operacionais, e da aplicabilidade de sua gestão por maturidade, é apresentada a Figura 20, baseada na estrutura COSO para governança corporativa.

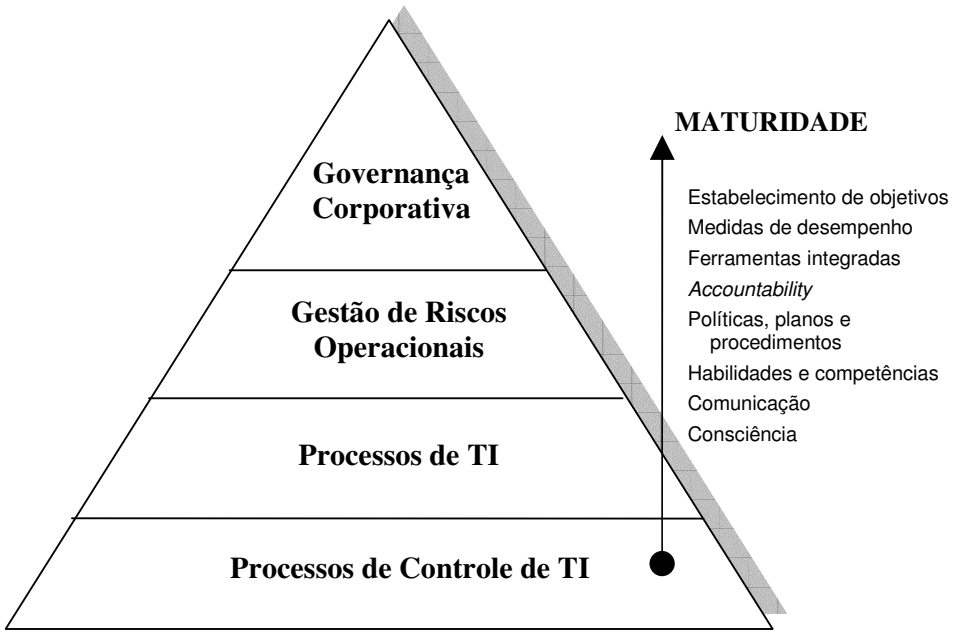


Figura 20 – Conformidade aos Princípios de Basiléia II (O autor)

A estrutura COSO tem em sua base o elemento *compliance* para o cumprimento às leis e regulamentações concernentes à organização. As recomendações do Novo Acordo de Basiléia (Basiléia II), não têm força legal, mas são boas práticas que estão balizando a implementação de estruturas internas para a gestão de riscos operacionais em instituições financeiras. Assim, a gestão por maturidade dos processos de controle e de tecnologia da informação dá suporte à organização para a mitigação de riscos operacionais, levando ao efetivo alinhamento entre os objetivos dos *stakeholders* estratégicos da organização e da governança de TI. Conduz, ainda, à conformidade aos princípios de Basiléia II, atendendo a critérios qualitativos para uso dos métodos avançados de alocação de capital para risco operacional.

4.5 Alta Confiabilidade

Este último item da análise de dados trata da investigação de características de alta confiabilidade, pressupostas em uma organização que conduz seus processos em condições de alto risco, em razão de sua tecnologia ou das conseqüências sócio-econômicas que um erro pode provocar. Para subsidiar esta análise, foram realizadas as entrevistas focadas nº 6, 8 e 11 do Quadro 15 (p. 87), com responsáveis pela operacionalização do processo de redesconto bancário, nos dois ambientes (DEBAN e DEMAB). Utilizou-se, também, a observação direta nesses ambientes operacionais e a pesquisa documental. A seguir, realiza-se a análise de conteúdo e a construção do mapa de associação de idéias, com base nos dados coletados.

4.5.1 Tipologia de Alta Confiabilidade

Segundo Rijpma (1997 *apud* Eede *et al.*, 2006), as organizações de alta confiabilidade (OAC) possuem sistemas complexos e fortemente acoplados. Roberts (1990) observa que falhas operacionais nessas organizações podem gerar graves conseqüências sócio-econômicas.

O ambiente tecnológico no qual o processo de redesconto bancário está inserido pode ser considerado complexo, de acordo com os atributos apresentados no Quadro 10 (p. 62). Existe proximidade entre os componentes do sistema que realizam o fluxo da operação (Figura 19, p. 96). Os grupos de serviço RDC e STR coexistem no ambiente de processamento de grande porte na sede da organização, com clara interconexão entre eles e o terceiro grupo de serviço, o SELIC, localizado no ambiente de processamento de grande porte na sede do Rio de Janeiro. Esta separação espacial existente traz, conforme o Quadro 10, uma característica linear ao sistema de redesconto bancário, que reduz sua complexidade.

Por outro lado, porém, essa segregação entre os componentes de sistema foi apontada como um grande fator para o aumento da complexidade operacional do redesconto, levando à criação de múltiplos controles interativos – outro atributo de complexidade – como pode ser observado na Figura 19. As mensagens trocadas entre os grupos de serviço segregados STR e SELIC são mensagens de controle, objetivando garantir o modelo 1 de liquidação "Entrega Contra Pagamento". As conexões entre os grupos separados espacialmente são conexões

compartilhadas. Para comunicar-se entre si, eles utilizam a infra-estrutura comum fornecida pela Rede do Sistema Financeiro Nacional (RSFN) para a troca de mensagens.

A mensageria envolve, ainda, criptografia de mensagens, acesso a bancos de dados, softwares gerenciadores de filas de mensagens, software de grupos de serviços, ambientes de homologação e produção, os quais têm substituições limitadas, reforçando a complexidade do sistema. A compreensão desse processo tecnológico, por parte das equipes responsáveis pelo processo de negócio, é boa, mas limitada. Quando alguma seqüência de eventos de processamento de mensagens não é compreensível imediatamente, as equipes de tecnologia da informação são imediatamente acionadas, para investigação mais aprofundada.

O grau de acoplamento ou interdependência (Quadro 11, p. 62) entre os sistemas é médio, uma vez que o processamento de uma operação se dá em uma ordem precisa e única para o alcance do resultado desejado. Contudo, esperas são permitidas, embora possam causar transtornos operacionais no emissor da mensagem e existem redundâncias disponíveis nos ambientes de TI do BCB, como servidores em local separado do centro de processamento principal (sítios de *backup*) e contingenciamento de mensagens.

Assim, considerando: (i) a análise da dicotomia entre sistemas complexos e lineares; (ii) o grau de acoplamento; e, ainda, (iii) o índice mínimo de disponibilidade do sistema de 99,8% (BACEN, 2002b), pode-se considerar o processo de redesconto bancário como um processo de negócio da tipologia de organização de alta confiabilidade.

O redesconto bancário é importante na gestão do risco sistêmico do SFN, que é missão institucional do BCB. Após a reestruturação do SPB, em 2002, criou-se o conceito de "hora de liquidação" de operações, conforme a Figura 17 (p. 92), levando à necessidade de liquidez financeira intradia por parte das instituições financeiras participantes do STR, que são bancos comerciais, bancos múltiplos com carteira comercial, caixas econômicas, bancos de investimentos (facultativo), câmaras de compensação sistemicamente importantes e câmaras de compensação não importantes sistemicamente (facultativo).

Essa condição, aliada aos volumes financeiros e de operações de redesconto bancário (Quadro 17, p. 95) permite considerar este processo de negócio como muito importante para o SPB e, desta forma, para a economia nacional.

4.5.2 Boas Práticas de Alta Confiabilidade

As habilidades para monitorar, detectar, prevenir e se antecipar a falhas operacionais (WEICK e SUTCLIFFE, 2001) foram observadas. Conferindo continuidade ao processo de negócio, nos dois ambientes envolvidos com o processamento de redesconto, equipes de monitoramento foram constituídas, com rodízio de turnos, das 6h às 13h e das 12h às 19h, para permitir a cobertura de toda a grade de redesconto (Figura 17, p. 92), com período de sobreposição de horário entre as equipes. Para detectar erros ou falha nos sistemas, as equipes possuem softwares de apoio, que permitem o acompanhamento do desempenho de processamento no fluxo de mensagens de redesconto (Figura 19, p. 96). Um panorama geral dos serviços de processamento é fornecido em dois telões dispostos na sala das equipes de monitoramento, facilitando a observação de anormalidades. Para antecipar possíveis falhas de processamento, modificações nos componentes de sistemas são disponibilizadas no ambiente de homologação, para que os participantes realizem testes.

A seguir, com auxílio de mapas de associação de idéias, são investigadas características de alta confiabilidade apresentadas na revisão da literatura. A grade de análise é composta por categorias que correspondem às boas práticas de OAC nos elementos de comunicação, tomada de decisão, estrutura, cultura e aprendizagem organizacional.

Para melhor disposição dos trechos de entrevista, as categorias de análise são apresentadas em linhas e não em colunas, como é originalmente indicado no uso do método. Para cada categoria, foram realizadas perguntas aos respondentes para verificar a presença ou não daquela característica. Os trechos de entrevista estão transcritos nas colunas associadas às categorias.

Os Quadros 21 a 24 contêm os mapas referentes às boas práticas observadas nos ambientes de monitoramento do processo de negócio, relativas aos elementos de comunicação, tomada de decisão e estrutura organizacional, cultura e aprendizagem. Em seguida, faz-se a análise das evidências e são explorados novos atributos considerados úteis para o modelo de maturidade do *framework* que serviu de base para a pesquisa.

Quadro 21 – Boas Práticas em OAC - Comunicação

	Resp 6	**Resp 8**	**Resp 11**
Entendimento de papéis e responsa-bilidades	Está bem definida nos documentos do banco. No ADM (...) Para cada departamento, para cada função dentro do departamento. São linhas gerais. Cabe ao coordenador fazer isso, cabe ao analista fazer isso, isso e isso. São atribuições do chefe de departamento. Atribuições que ele pode delegar (...) As rotinas têm normativos do departamento, passo a passo. É o que a gente chama de MPR. Inclusive no MPR trata-se de comunicação.	Você tem reunião de coordenação, reunião com bancos, nivelamento de monitores. Você tem um processo que busca nivelar a informação e procedimentos com todo mundo (...) Todas as atividades foram mapeadas, ao longo da manhã, do início da tarde, e de fechamento. E aí a equipe que assume aqui tem estas atividades, independente de quem ela está se submetendo hierarquicamente (...) E tudo o que acontece aqui é trocada a comunicação entre os dois turnos	Sempre estamos conversando (...) Eu acho muito ruim a instituição ligar e dizer: 'Ah! Mas eu falei com o pessoal da manhã...' e o cara da tarde não saber do que se trata (...) Os encarregados da manhã devem passar para os comissionados da parte da tarde tudo o que aconteceu pela manhã
Discussões para melhorias	As melhorias no sistema são decididas na medida das demandas tanto dos departamentos, quanto das divisões quanto dos participantes (...) A área de tecnologia identificou uma tela que estava sobrecarregando o sistema e pediu para mudar (...) Às vezes as regionais descobrem alguma coisa que tem que ser melhorada. Então a gente estimula eles a discutirem e depois passar para a gente (...) Todo ano a gente faz uma reunião com os participantes, bancos e câmaras (...)	Toda a equipe que trabalha no monitoramento deve questionar e apresentar proposta para melhorar (...) Eles construíram um modelo de acompanhamento de intradia de banco, que veio de uma regional aí... o pessoal gostou	Sempre estamos estudando o sistema para ver se a gente consegue melhorar
Espaços de "não-punição"	Geralmente os chefes aceitam, coordenam. Alguns a primeira reação é de explodir; outros já amenizam e depois vem a bronca; ou dão a bronca antes. Depende. Geralmente a pessoa quando identifica o erro já fala na hora, independente do nível. Todo mundo tem consciência aqui de que um erro pode gerar prejuízo	Tem. A seqüência operacional nessa hora é: houve o erro, identifica-se o erro, conserta-se o erro, tá certo? Após consertar o erro, não quero saber quem foi. Deu pepino, não me interessa. Não quero desculpa agora. Vamos correr para consertar o problema, qualquer que seja. Agora vamos avaliar o processo para saber o que houve. Da próxima vez faz assim, assim. Não há, em princípio, uma regra para punir...Isso aí não (...)	Se tem um quase-erro ou erro, a gente reconhece, tenta consertar. A gente tem aqui muita coisa de conferência (...) A gente vai buscando a melhoria (...) A chefia vai chamar a atenção? Claro que vai, mas como todo ser humano

Fonte: Pesquisa de campo

Quadro 22 – Boas Práticas em OAC – Estrutura Organizacional e Tomada de Decisão

	Resp 6	**Resp 8**	**Resp 11**
Varia de estilo burocrático a colegiado, de acordo com a situação	Na decisão de prorrogação do horário do STR, tanto o Deban quanto o Demab só comunicam um ao outro (...) não questiona o outro o motivo da prorrogação. É decisão das chefias e são acatadas (...) O que pode acontecer é ter um caso imprevisto e alguém ter que decidir na hora (...) O monitoramento é colegiado e o departamento é burocrático (...) Às vezes tenho que tomar a decisão e pergunto: "pessoal, o que vocês acham?" (...) Às vezes algumas coisas já estão definidas, estão claras, não tem abertura para questionar (...) Há liberdade para cada um se expressar e ajudar na tomada de decisão (...) Então aquela estrutura matricial, o monitoramento é assim. Só funciona porque é assim	Colegiado! Inclusive, o que a gente pede é que ninguém fale muito baixo ao telefone. Para que ninguém tome uma decisão sozinho. Por isso que tem aquele jeitão de sala de operações, de controle, para ouvir o que o outro está falando.	Se é uma coisa que a gente acha que é muito grave, nós já avisamos a nossa chefia, que aí entra todo mundo.
Em situação de emergência, experiência precede posto	Em um momento de crise, por exemplo, eu tenho que ter todas as informações da minha alçada, passar a minha opinião para o chefe para ele decidir também (...) Algumas vezes a chefia pergunta qual a tua opinião, outras ela tem conhecimento de coisas que o operacional não conhece e ela toma a decisão com base neste conhecimento. A experiência pesa. (...) No momento de crise, orientação veio de cima, faça, depois você questiona. A não ser que vá causar prejuízo, aí você fala.	Experiência. Nunca posto. Você tem sempre um cara... é normal nesse tipo de time, você tem alguém que tem melhor posição para coordenar. Porque crise, o problema é você ter coordenação. Porque começa todo mundo a bater cabeça, a bater cabeça. Nessa hora você tem um cara... o que você procura fazer é nomear, para evitar o choque, é você dar prevalência no posto àquele cara que tem aquela característica de administração de crise.	Eu diria a você que é a experiência. O poder de decisão passa a ser de todo mundo, mas quem fecha é o chefe de divisão ou de departamento (...). A gente pode até resolver por experiência, mas quem tem que bater o martelo é a chefia (...) É claro que o posto diz mais alto, porque senão... pra que hierarquia?

Fonte: Pesquisa de campo

Quadro 23 – Boas Práticas em OAC – Cultura

	Resp 6	**Resp 8**	**Resp 11**
Integração de novos membros	A gente passa os manuais de procedimentos para ele dar uma olhada. Depois, uma câmara para ele monitorar, geralmente a menor. Sempre tem alguém perto dele. Ele está fazendo, mas tem alguém responsável por trás olhando, também. E aí vai acrescentando atividades, aos poucos	Primeiro é a brincadeira. Mas depois o cara passa por todos os postos, ele é colocado do lado de um mais novo. Até para melhorar o treinamento do mais novo (...) As posições, nas mesas são trocadas com uma certa constância para integrar todo mundo (...) Importa muito o perfil das pessoas. Primeiro, tem que gostar de falar. Não pode ser introspectiva. Você precisa saber o que o cara está falando. Ele precisa ter coragem de falar: errei! Tô fazendo uma bobagem, o que vocês acham? Então você tem que compartilhar as suas experiências ali. Ele tem que ter... poder de concentração para trabalhar em ambiente que tem muita gente falando.	A gente sempre quer passar o melhor do sistema. Todos nós gostamos do que fazemos (...) A pessoa tem que estar atenta, percebendo todo o movimento do mercado. Tem que ter um *feeling* para isso (...) Nós uma vez recebemos um funcionário, ensinamos... mas ele não conseguia atender telefone.
Mesmo em situação de rotina há algo a apreender	O monitoramento é 80% rotina e 20% novas situações (...) todo o dia tem uma coisa nova: funcionamento de sistema de pagamentos fora do país, mudança de telas (...) Todo dia tem pesquisa. Você entra no site do BIS, no do Banco Central Europeu, você vai ver coisa nova com relação ao sistema de pagamentos	Hoje a ocorrência de problemas é cada vez menor, e quanto menor a freqüência, maior vai ser o impacto. Temos que manter a equipe treinada para numa situação de problema, conseguir ir de 0 a 100 em 5 segundos	A gente faz a rotina aqui. Mas a pessoa fica estudando, tem coisas que a gente sai pesquisar para depois passar para a chefia. A gente está sempre em melhoria.
Consciência de que o sistema pode falhar	A preocupação com falhas é constante, mesmo assim erros acontecem	A possibilidade existe, mas aquela equipe que está lá ... eles têm uma incrível capacidade de criar cenários que varrem praticamente todas as possibilidades. Isso ficou muito reduzido. Mas quando não passa pelo crivo daquela equipe ...	Vamos ficar atentos, porque no dia que você não fica, pode acontecer alguma coisa. Já está no sangue da gente (...) qualquer mexida que entra na produção a gente fica atento (...) Isso é máquina, feito por humano

Pequenos erros são levados a sério	Uma coisa que a gente orienta aqui é sempre que a gente tiver ao telefone, falar alto. Todo mundo que estiver ao telefone, está sendo percebido por quem está perto. Se a gente perceber que está fornecendo uma orientação errada, a gente interrompe, corrige a informação para passar correto (...) O que é o pequeno erro? O pequeno erro é gerado por informação errada.	Uma vez eu fiz um teatro [fez de conta que um pequeno erro ocorrido havia gerado uma fraude] Normalmente eu chego brincando com todo mundo. Não dei bom dia pra ninguém. E chamei os 3: um que faz, um que confere e outro que libera. Contei que era uma fraude. Os 3 ficaram brancos. Teve um que começou a tremer...	Não tem grau de excelência aqui. Erro é erro. Tem que ser bem tratado
Normas balizadoras	Você tem um plano a seguir. Existe um roteiro para a ação (...) Eu tenho no computador, mas se você olhar em todas as mesas tem o MPR (Manual de Procedimentos e Rotinas) impresso (...) Que atitude eu tomo? Então é bom ter uma coisa escrita, com um linguajar padrão	O pessoal tem todo um roteiro. Como faz com o meio circulante se acontece isso e isso... Inclusive tem um manual de redesconto que foi disponibilizado para os monitores	Existem normas. Primeira coisa que a gente faz: tem que ler o regulamento do sistema. Tem que saber o que você pode fazer. Conhecer quais as instituições, quem pode fazer o que. Esse aqui é o manual do usuário. A gente esmiuçou o regulamento para cá. É a nossa bíblia
Comprometimento com falhas em todos os níveis	Numa situação em que o banco não pagou a Compe (...) procurei o gerente, celular desligado. Liguei para a casa dele (...) Liguei para o chefe de departamento (...) Eu vou ligar para o adjunto	Sim todo mundo. O chefe de departamento, o chefe adjunto. Ele está com a preocupação de que aquilo funcione o tempo todo	Eu acredito que sim.. O pessoal sabe que eles estão lá para evitar falha

Fonte: Pesquisa de campo

Quadro 24 – Boas Práticas em OAC – Aprendizagem

	Resp 6	**Resp 8**	**Resp 11**
Sistema de trabalho intensivo em conhecimento	Por mais que você leia, nunca é suficiente, porque não é uma pessoa produzindo, não é um órgão produzindo. São vários produzindo e mandando.		A gente teve que conhecer muitas coisas. Tivemos que aprender a mensageria. O que envolvia. Os campos, tudo isso, para integrar nosso sistema dentro do SPB.
Autodesenvol-vimento e Autodiagnós-tico	A gente está fazendo um estudo sobre os sistemas de pagamentos, liquidação em tempo real no resto do mundo. A pessoa pega um sistema, estuda e apresenta para todo mundo. Então há uma aprendizagem individual que é maior que a coletiva (...) E a própria questão operacional em si, sempre que alguém percebe alguma coisa, é avisado imediatamente para todo mundo	As idéias são sempre submetidas a bombardeio. Todo mundo participa. Você houve as regionais. A crítica é aberta. Mesmo a destrutiva. Se tiver consenso, quando se concorda, o cara tem o mérito.	Quando aparece uma norma, um comunicado no sistema que vai mudar alguma coisa, a gente senta, vamos conversar com todo mundo. Depois a gente escreve em cima do consenso, as informações foram passadas para todo mundo (...) Aqui a gente pergunta. Por que é assim, é assado. Hoje mesmo, eu estava perguntando o que faz a operadora e a seguradora de saúde, regulamentarmente.
Reavaliação de pressupostos, tarefas e decisões	O MPR, por exemplo, é revisado, anualmente, duas vezes (...) Durante a crise é feito um relatório de todos os procedimentos adotados. Vai para a chefia. Há questionamentos. Vai se criando um histórico, uma cartilha (...) A tomada de decisão tem que ser discutida. Simplesmente tomar uma decisão porque você acha que é isso, ou porque está escrito que é isso. Mesmo que está escrito avalia-se aquilo	Decisões são mudadas no meio do caminho. Antes de você anunciar a decisão tem a discussão. Então a decisão nunca é de um cara só. (...) O pessoal está o tempo inteiro mudando, refazendo, buscando melhorar.	Existe sempre o questionamento de porquê é assim
Confiabilidade concomitante à flexibilidade	Ambos. Não tem como. Eu não posso deixar de ser confiável, por uma questão de valores. Eu não posso deixar de ser flexível pelas situações inesperadas que acontecem (...) Mas confiabilidade primeiro, flexibilidade em segundo.	Tem que ter confiabilidade. A gente tá mexendo com dinheiro. Eu tenho que ter regra firme. Procedimento padrão. Eu não diria que em primeiro plano estaria a flexibilidade. Flexibilidade da equipe, sim. Organize sua vida sempre sabendo que você poderá vir pela manhã ou à tarde.	Confiabilidade, acima de tudo (...) Flexibilidade vem logo depois (...) Você é flexível para manter a confiabilidade (...) Acho que elas andam de mão dada, mas em primeiro lugar a confiabilidade

Organizar, aprender, desorganizar e reaprender	Na verdade você vai ter um processo de reorganização constante. De reestruturação constante. A gente está estudando coisas interessantes para aplicar aqui. Se forem aplicadas, vai ter que reorganizar. Então é um processo constante (...) Não só a reorganização de trabalho, mas de estrutura mesmo. Estrutural!		Como a gente teve com o SPB. A gente teve que apreender e mudar. E fomos apreender. E reorganizar. Ao mesmo tempo. É um ótimo exemplo. Nós tivemos isso aqui vivamente. Três ficavam nessa salinha aqui, estudando, testando, depois ia trocar idéia. De tarde outro grupo. Ainda tínhamos que tomar conta do sistema on-line. Então houve a transição do organizado, do aprendizado e da desorganização para se organizar (...) Foi uma revolução. A gente se deu conta de que todo mundo estava junto, apreendendo

Fonte: Pesquisa de campo

Esta etapa da coleta de dados ocorreu em três momentos distintos, o que não permitiu a interanimação dialógica entre os respondentes acerca das características organizacionais apresentadas nos mapas de associação de idéias. Mesmo assim, a disposição dos trechos das entrevistas permite uma aproximação de um possível diálogo, embora a argumentação e contra-argumentação certamente aumentariam a produção de sentidos e, conseqüentemente, as evidências buscadas.

No Quadro 25, busca-se explorar a associação das idéias apresentadas, bem como relacionar cada uma das categorias de análise aos atributos de maturidade descritos no modelo COBIT, que são: consciência; comunicação; políticas, planos e procedimentos; ferramentas; automação; habilidades; competência; responsabilidades; prestação de contas; estabelecimento de objetivos; e medidas de desempenho.

Quadro 25 – Boas Práticas em OAC e Atributos de Maturidade

Categoria	Associação de Idéias	Maturidade COBIT
Comunicação: 1.Entendimento de papéis e responsabilidades	1.Há normas que estabelecem diretrizes gerais e procedimentos internos dentro das unidades administrativas. 2.Há reunião de grupos para nivelar informações e procedimentos. 3.As relações interpessoais auxiliam na condução das responsabilidades. Observa-se a pautação das atividades em normas definidas e busca de participação das pessoas no auxílio mútuo para cumprimento de responsabilidades.	Consciência Comunicação Procedimentos Responsabilidades
Comunicação: 2.Discussões para melhorias	1.Ocorrem reuniões interorganizacionais para sugestões de melhorias nos sistemas. 2.O centro principal de monitoramento do processo de negócio é auxiliado pelas regionais na busca organizacional por melhorias. 3.O foco local nas atividades cotidianas também busca melhorias. As sugestões para melhoria ocorrem nos âmbitos interorganizacional, organizacional e local.	Políticas Planos Comunicação
Comunicação: 3.Espaços de "não-punição"	1.Sempre ocorre a bronca. 2.O objetivo principal é consertar o erro. A avaliação da situação é impessoal. 3.Chamar a atenção é natural. A ocorrência de erros pode gerar constrangimento, o que pode diminuir as chances de revelação de situações de erro ou quase-erro.	Habilidades Competências Prestação de Contas Responsabilidades
Estrutura organizacional: 4.Varia de estilo burocrático a colegiado, de acordo com a situação	1.O departamento é burocrático, mas o monitoramento é matricial, prevalecendo o estilo colegiado. 2.O objetivo é que ninguém tome, sozinho, decisões. 3.Toda a chefia é avisada para participar na decisão. A estrutura interna matricial fornece condições para decisões colegiadas. Sempre que necessária a participação de postos superiores, o estilo burocrático prevalece.	Políticas Responsabilidades

Tomada de decisão: 5.Em situação de emergência, experiência precede posto	1.A tomada de decisão ascende na hierarquia, com embasamento pela experiência. 2.A experiência conduz ao posto. 3.Quem decide é a chefia. A experiência é sempre respeitada, mas a decisão final é do posto, que tende a ser o mais experiente.	Políticas Responsabilidades
Cultura: 6.Integração de novos membros	1.O compartilhamento de artefatos e padrão de pressupostos básicos é evolutivo. 2.A integração inicial é a descontração. Mas a aceitação no grupo depende do perfil para o trabalho. 3.O grupo se sente orgulhoso em receber um novo membro, que deve ter o perfil para a integração. A adaptação de novos membros é favorável, mas o fundamental é ter o perfil para as atividades do grupo.	Habilidades Competência
Cultura: 7.Mesmo em situação de rotina há algo a apreender	1.Sempre há algo a aprender com relação ao trabalho. Sempre há pesquisas na área. 2.A equipe deve estar preparada para enfrentar situações de emergência a qualquer hora. 3.Novos conhecimentos são passados para a chefia. O trabalho é mesmo de rotina, mas há consciência de que o conhecimento na área de negócio avança e é preciso atualizar-se e compartilhar novidades. A equipe tem que estar sempre bem preparada para situações de estresse.	Habilidades Competência
Cultura: 8.Consciência de que o sistema pode falhar	1.Erros acontecem. A preocupação é constante. 2.Mas a probabilidade é muito baixa. A equipe avalia todos os cenários possíveis. 3.Mas não se pode descuidar. Máquinas são feitas por humanos. Há consciência de que as máquinas podem falhar, já que são concebidas e construídas por seres humanos, entretanto, o esgotamento de cenários possíveis de uso torna muito baixa a probabilidade de erros em sistemas maduros.	Ferramentas Automação

Cultura: 9.Pequenos erros são levados a sério	1.Pequenos erros, como instruções ao telefone, devem ser evitados na origem. 2.Quando ocorre um pequeno erro, ele deve ser superdimensionado para mostrar o que poderia acontecer. 3.Todos os erros devem ser tratados iguais. Pequenos erros devem ser evitados e relacionados a conseqüências graves que poderiam ocorrer.	Procedimentos Responsabilidades
Cultura: 10.Normas balizadoras	1.Elas estão disseminadas na equipe. 2.Todos os passos das atividades estão detalhados. 3.Todos os regulamentos devem ser conhecidos. É essencial o detalhamento das atividades, e deve ser do conhecimento de todos os membros da equipe.	Procedimentos Responsabilidades
Cultura: 11.Comprometimento com falhas em todos os níveis	1.Deve haver pró-atividade para que toda a hierarquia tenha conhecimento de exceções e haja o comprometimento em todos os níveis. 2.Os chefes superiores estão preocupados com o funcionamento contínuo do processo. 3.Os chefes estão sempre vigilantes. Os chefes estão envolvidos com a continuidade operacional, mas é necessário buscar o seu comprometimento também.	Políticas Responsabilidades
Aprendizagem: 12.Sistema de trabalho intensivo em conhecimento	1.São várias as fontes de produção de conhecimento na área. É impossível acompanhar tudo. 2.- 3.Foi necessário aprender muitos conceitos técnicos em virtude da mudança no processo de negócio. Tanto o conhecimento dos aspectos de negócio quanto dos aspectos técnicos dotam a atividade de monitoramento de necessidade de contínuo aperfeiçoamento.	Habilidades Competência
Aprendizagem: 13. Autodesenvolvimento e Autodiagnóstico	1.O autodesenvolvimento e o autodiagnóstico se dão no plano individual e também no coletivo. 2.Ocorre o autodiagnóstico crítico. As idéias são sempre criticadas, em busca do consenso e mérito. 3.Busca-se sempre o consenso coletivo. A organização aprende com a busca, no plano individual, por novos conhecimentos e avaliação crítica de propostas.	Habilidades Competência Medidas de desempenho

Aprendizagem: 14.Reavaliação de pressupostos, tarefas e decisões	1.As decisões tomadas são questionadas e validadas para consubstanciar os procedimentos adotados. 2.Mesmo durante a tomada de decisão, ela pode ser alterada. Ela é discutida pelo grupo. 3.Os porquês existentes são questionados. Os pressupostos existentes são reavaliados pelo grupo, que os questiona, em um circuito duplo de aprendizagem.	-
Aprendizagem: 15.Confiabilidade concomitante à flexibilidade	1.Ambas. Confiabilidade é a característica principal que define o processo. As situações inesperadas exigem flexibilidade. 2.As normas são feitas para dar confiabilidade em primeiro lugar. Depois vem a flexibilidade, principalmente de equipe, em função dos turnos de monitoramento. 3.Em primeiro lugar vem a confiabilidade. Mas a flexibilidade, que vem em seguida, ajuda a manter a confiabilidade. O objetivo principal da equipe é a confiabilidade. A flexibilidade estão em um segundo plano muito próximo, inclusive para sustentar a confiabilidade. Busca-se ambas.	Estabelecimento de objetivos Medidas de desempenho
Aprendizagem: 16.Organizar, aprender, desorganizar e reaprender	1.O processo de reorganização do trabalho é constante, inclusive da estrutura que o suporta. 2.- 3.Houve essa experiência e é um ótimo exemplo. Com a necessidade de manter em funcionamento o sistema e ao mesmo tempo prepará-lo para incorporar novos requisitos de mensageria. Foi uma revolução. Apesar de antagônicos, os processos de organizar e aprender são essências para a formação de hábito concomitante com a descoberta, para então permitir a reorganização.	-

Fonte: Análise dos Quadros 21 a 24 e do modelo genérico de maturidade COBIT

A análise interpretativa das práticas discursivas, realizada no último quadro, sugere a existência das boas práticas de alta confiabilidade nos ambientes de monitoramento, responsáveis pela operacionalização do processo de redesconto bancário e também pela melhoria contínua desse processo de negócio.

Contudo, algumas características não foram plenamente evidenciadas, como: a promoção de espaços de "não-punição" para diminuição de incertezas e análise de situações de falha ou quase-falha; em situação de emergência, a experiência não precede o posto, mas fundamenta a tomada de decisão.

Das 16 categorias de boas práticas, 14 podem ser relacionadas a atributos de maturidade de processos do modelo COBIT para governança de tecnologia da informação. A terceira coluna do Quadro 25 faz esse relacionamento.

As duas categorias do elemento aprendizagem que não constam no referido modelo de maturidade são: nº 14 – "Reavaliação de pressupostos, tarefas e decisões" e nº 16 – "Organizar, aprender, desorganizar e reaprender", relativas às organizações de aprendizagem.

Purser e Pasmore (1992, *apud* Weick e Westley, 1996) observam que as organizações "aprendem a aprender" ao criticar seus pressupostos, suas crenças, tarefas, decisões e problemas estruturais. Weick e Westley (1996, p.369) dizem que o ponto de aprendizagem ótimo está na justaposição entre ordem e desordem, sendo esses pontos identificados como aprendizagem de circuito simples e aprendizagem de circuito duplo. O primeiro enseja a formação de hábito, a redução de desvios, a aprendizagem reativa. O segundo, a descoberta, a exploração, a aprendizagem pró-ativa.

O modelo COBIT implementa o circuito único de aprendizagem, com orientações para controle, redução de desvios e mitigação de riscos em seus processos de tecnologia da informação, conforme ilustrado na Figura 12 (p. 57). Já os princípios de governança corporativa, mostrados na Figura 6 (p. 43), envolvem a comunicação bidirecional nos níveis organizacionais e a realização de *feedback* para os níveis superiores, responsáveis pela formulação de objetivos estratégicos e políticas da empresa, caracterizando o circuito duplo de aprendizagem, como exibido na Figura 14 (p. 65).

Desta forma, a maturidade dos processos de governança de tecnologia da informação poderiam refletir esta adaptação no modelo, que passaria a permitir o questionamento dos pressupostos básicos, com propósito de melhorá-los, passando este atributo a figurar entre os atributos já existentes no modelo genérico de maturidade, possivelmente caracterizando o nível gerenciado ou otimizado de maturidade de processo. A Figura 21 ilustra esta proposição.

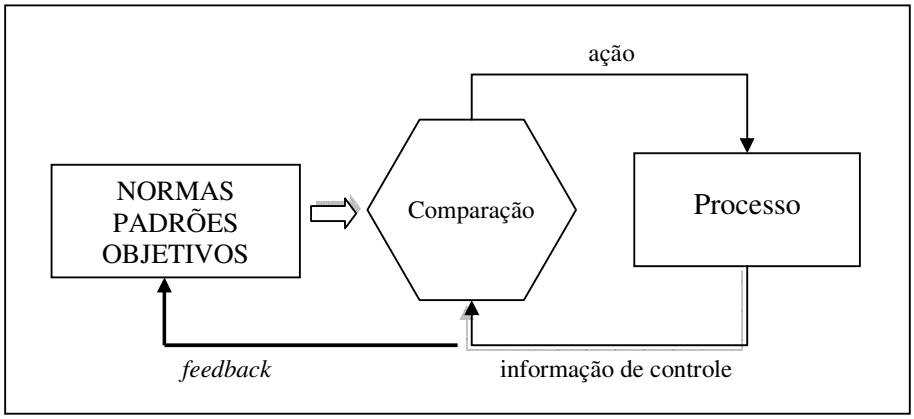


Figura 21 –Adaptação no modelo COBIT

Fonte: O autor, a partir da análise de dados e de ITGI, 2007b, p. 14

Na Figura 21, o incremento da ação de *feedback* permitiria a justaposição entre os circuitos simples e duplo de aprendizagem, cujo ponto ótimo é caracterizado pela presença concomitante dos "processos antagônicos" (WEICK e WESTLEY, 1996, p.369) organizar e aprender. Assim, a boa prática de alta confiabilidade nº 16 – "Organizar, aprender, desorganizar e reaprender" estaria também contemplada no modelo adaptado.

Este item da análise de dados permitiu comparar as boas práticas de organizações de alta confiabilidade com as boas práticas prescritas no modelo COBIT para governança de tecnologia da informação. Verificou-se que a gestão da maturidade dos processos de tecnologia da informação pode ser incrementada com a inclusão de elementos de aprendizagem organizacional, os quais tendem a fazer parte dos ambientes de organizações de alta confiabilidade.

A última seção deste trabalho destina-se às considerações finais.

5 CONSIDERAÇÕES FINAIS

Este estudo é uma contribuição teórico-empírica nas áreas de conhecimento de governança corporativa, governança de tecnologia da informação, gestão de processos por maturidade, organizações de alta confiabilidade e gestão de riscos operacionais. O risco operacional tem componentes relacionados a falhas de tecnologia da informação, deficiência em processos e inadequação de recursos humanos e passou a fazer parte das recomendações do Comitê da Basiléia II para o setor financeiro mundial.

A unidade de análise foi o processo de negócio de redesconto bancário, operacionalizado na Diretoria de Política Monetária do Banco Central do Brasil. Foi possível verificar relacionamentos entre processos de governança de tecnologia da informação (processos de TI e processos de controle) e a maturidade para mitigação de riscos operacionais, bem como investigar a presença de características de alta confiabilidade no ambiente de negócio relacionado ao processo de redesconto bancário.

Esta pesquisa adotou a estratégia de estudo de caso simples, com abordagem mista para análise de dados. A coleta de dados foi conduzida com informantes-chaves nas áreas de negócio, de tecnologia da informação e de auditoria interna. Foram realizadas entrevistas espontâneas focadas, aplicação de questionário eletrônico, observação direta e pesquisa documental. Para a análise de dados, utilizaram-se os métodos qualitativos denominados análise de conteúdo e mapa de associação de idéias. Como métodos quantitativos, foram adotadas a estatística descritiva e a análise de freqüência.

Em síntese, é possível afirmar que os objetivos dessa dissertação foram atingidos, na medida em que as questões de pesquisa foram respondidas ao longo do quarto capítulo. Para permitir a investigação do problema de pesquisa, inicialmente o processo de negócio foi descrito, o que serviu de base para o encadeamento das questões descritas a seguir.

A primeira questão de pesquisa envolveu a **identificação de riscos operacionais** no processo de redesconto bancário. Foram explorados os aspectos de TI que suportam o processo, gerando dois tipos de riscos operacionais: os presentes na rotina diária do processo de negócio, já observados ao menos uma vez; e os risco operacionais pouco prováveis, circunstanciais ou hipotéticos. Destinado a dar liquidez no âmbito do Sistema de Pagamentos

Brasileiro, o redesconto bancário é operacionalizado em dois ambientes interdependentes de processamento de dados, um em Brasília e o outro no Rio de Janeiro, sede da administração do Sistema Especial de Liquidação e de Custódia (Selic). Ao todo, foram identificados 39 riscos operacionais.

A segunda questão analisou o grau de contribuição dos processos de governança de TI para a mitigação dos riscos operacionais encontrados. Com base na revisão da literatura, foram selecionados para o estudo 6 **processos de TI** do *framework* COBIT. Eles foram avaliados por profissionais da área correlata, que apontaram a importância de cada processo para a mitigação dos 39 riscos operacionais, em uma escala intervalar do tipo Likert de 5 pontos. A partir da análise quantitativa, verificou-se que todos os processos contribuem fortemente para a mitigação dos riscos operacionais, na seguinte ordem: Continuidade de Serviços, Avaliação e Gestão de Riscos, Segurança de Sistemas, Gestão de Dados, Gestão de Projetos e Gestão de Recursos Humanos de TI.

Para avaliar se os 6 processos de TI tinham o mesmo grau de importância para mitigação de riscos nos dois grupos identificados, realizou-se o teste não-paramétrico U de *Mann Whitney,* no qual foi constatado que os processos de Gestão de Projetos e Segurança de Sistemas têm maior impacto na mitigação dos riscos operacionais identificados ao nível hipotético do que aqueles da rotina diária.

A terceira questão de pesquisa implicou na investigação da importância de outros dois processos de governança de tecnologia da informação para mitigação de riscos operacionais: os **processos de controle** Promoção de Governança de TI e Monitoramento e Avaliação de Controles Internos. A coleta de dados foi realizada junto a profissionais de auditoria interna, uma vez que esses processos não estão diretamente relacionados ao processo de redesconto nem a riscos operacionais específicos, mas a governança corporativa e ao sistema de controles internos. Apoiada no modelo COBIT, os órgãos de controle da União vêm promovendo a governança de tecnologia da informação, por meio de auditorias externas e recomendações. Em linha com esta prática, a governança de TI está sendo conscientizada e comunicada na organização, o que caracteriza os níveis iniciais de maturidade do processo. De maneira similar aos requisitos para governança corporativa, a promoção de governança de TI busca a criação de uma estrutura organizacional, a responsabilização e o estabelecimento de papéis para a sua consolidação, indo ao encontro de princípios do Basiléia II para a gestão do risco

operacional. Assim, o processo Promoção de Governança de TI assume papel estratégico no modelo de boas práticas. Atua, indiretamente, como suporte fundamental na mitigação de riscos operacionais.

O foco das atividades de controle interno tem se ampliado, passando a incluir a gestão de riscos além da verificação de conformidade a regulamentações legais. O processo de Monitoramento e Avaliação de Controles Internos atua no sistema de controle internos, que envolve o ambiente de controle, a avaliação de riscos, as atividades de controle, a informação e comunicação e as atividades de monitoramento. O monitoramento e o controle interno permeiam todos os processos de tecnologia da informação, em busca de correção de desvios dos objetivos estabelecidos e *feedback* para a gestão de riscos operacionais. Um dos objetivos dos controles internos é a eficiência operacional.

Para responder à quarta pergunta de pesquisa, referente à aplicabilidade dos **modelos de maturidade** para a gestão de processos, foi elaborado um instrumento de campo em forma de questionário eletrônico para permitir a simulação em tempo real de modelos simplificados de maturidade de processos e para validar os resultados apresentados. A média geral de maturidade de processos apontou para o nível "Definido" de maturidade, intermediário na escala geral, corroborando outras pesquisas afins. Foi considerada válida a aferição da maturidade de processos por meio de atributos como consciência e comunicação, procedimentos, automação, prestação de contas e medidas de desempenho. A gestão de processos por maturidade mostrou-se útil para a organização, tanto no autodiagnóstico inicial quanto no acompanhamento de medidas de evolução e alcance de metas.

A investigação da quinta e última pergunta de pesquisa – quais os fatores de maturidade para governança de TI que podem ser considerados importantes nas **organizações de alta confiabilidade**? – implicou na validação de pressupostos desta tipologia de organizações, que se caracterizam pela complexidade tecnológica e conseqüências sócio-econômicas que podem surgir em conseqüência de um erro operacional. Esta análise foi conduzida nos centros de monitoramento envolvidos na operacionalização do redesconto bancário, onde foram diagnosticados atributos de complexidade tecnológica, de acoplamento de sistemas e de importância do processo de negócio para o Sistema Financeiro Nacional.

Boas práticas de alta confiabilidade relacionadas a elementos organizacionais – comunicação, tomada de decisão, estrutura, cultura e aprendizagem organizacional – foram avaliadas pelos respondentes, e com o auxílio de mapas de associação de idéias buscou-se a sua validação no contexto organizacional. Verificou-se, também, que as boas práticas de alta confiabilidade estão presentes nas boas práticas do modelo de maturidade de processos adotado neste estudo, com exceção de algumas categorias de análise referentes à aprendizagem. Desta forma, evidencia-se a possibilidade de incremento desses modelos, justapondo aprendizagem de circuito simples e aprendizagem de circuito duplo.

Em função da pesquisa empírica, então como a maturidade nos processos de governança de tecnologia da informação e as características de alta confiabilidade contribuem para a mitigação do risco operacional em instituições financeiras?

Em primeiro lugar, observa-se que as características de alta confiabilidade estão para a área de negócio, assim como os processos de tecnologia da informação estão para a área de sistemas e os processos de controle de governança de TI, para a área de auditoria interna e também externa. Eles são complementares na gestão de riscos operacionais.

A revisão da literatura permite a seleção de importantes processos de TI para mitigação de riscos operacionais, de acordo com análise de cenários, recomendações do Basiléia II para instituições financeiras e constatações sobre a aplicabilidade de modelos de governança de tecnologia da informação, como o *Control Objectives for Information and related Technology – CobiT*, o qual serviu de base para a pesquisa.

Os processos de Continuidade de Serviços, Avaliação e Gestão de Riscos, Segurança de Sistemas, Gestão de Dados, Gestão de Projetos e Gestão de Recursos Humanos de TI contribuem para a gestão de riscos operacionais em seu componente de tecnologia da informação, principalmente, e de deficiência em recursos humanos. O terceiro fator de risco operacional, a inadequação de processos, tende a ser mitigado a partir da evolução dos níveis de maturidade dos processos.

Os níveis de maturidade refletem atributos que vão desde a conscientização até o uso de métricas de desempenho para a gestão. Um grande desafio para essa evolução está relacionado à institucionalização de processos, que é demarcada pelo nível “definido” de

maturidade. Neste estágio, os processos passam do indivíduo para a organização, tornando-os impessoais e incentivando a racionalidade formal, burocrática.

Esta evolução de maturidade é promovida pelos processos de controle de governança de tecnologia da informação, que é uma extensão da governança corporativa, só que em um ambiente mais focado. A criação de estruturas organizacionais, a definição de papéis e o apoio de lideranças são pilares fundamentais para que a governança de tecnologia da informação tenha seus objetivos alinhados às metas da organização e seus processos consigam alcançar níveis maiores de maturidade. O monitoramento e a avaliação de controles internos com foco em risco é um processo tipicamente de controle, no sentido de que busca influenciar ações em prol da gestão de riscos operacionais no ambiente de TI, consolidando um ambiente de controle, cujos objetivos inclui a eficiência operacional.

No entanto, a gestão de processos por níveis de maturidade, apesar de importante, parece ainda um pouco distante da realidade organizacional. Este tipo de gestão reflete níveis superiores de maturidade, como o "gerenciado" e o "otimizado", que adotam métricas de processos para o seu aperfeiçoamento contínuo. Pesquisas internacionais apontam para processos de TI entre os níveis "repetido" e "definido".

Em virtude do aumento da interdependência e da complexidade tecnológica utilizada para resolver problemas cada vez mais complexos do ambiente de negócio, as boas práticas de alta confiabilidade, por sua vez, contribuem para a gestão do inesperado – eventos de risco operacional, independentemente de sua probabilidade, que passam a fazer parte do cotidiano organizacional. Organizações que conseguem aliar às boas práticas de governança de TI as boas práticas de comunicação, tomada de decisão, cultura e aprendizagem para mitigação de riscos têm maiores chances de alcançar a eficácia da gestão de riscos operacionais.

Em sistemas de trabalho intensivos em conhecimento, como é a área de tecnologia da informação, a aprendizagem de circuito único justaposta à aprendizagem de circuito duplo torna os modelos prescritivos mais adequados a sua própria evolução. A constante validação de pressupostos, tarefas e decisões – portanto uma possibilidade de mudança cultural – é uma característica presente em processos de negócios em que a ocorrência de falhas pode gerar graves prejuízos sócio-econômicos.

Essa generalização analítica possui algumas limitações. Inicialmente, a própria racionalidade limitada e viés do pesquisador podem ter causado distorções no processo contínuo de interpretação e readaptação de instrumentos de pesquisa, que faz parte de um estudo de caso. Para tentar contrapor essa limitação, foi adotado o protocolo sistemático para coleta de dados, apesar da adaptatividade necessária em pesquisas qualitativas.

Em razão da necessidade de simplificação dos modelos de maturidade de processos, a formulação do questionário eletrônico para simulação desses modelos incluiu algumas assertivas que são compostas e outras que usam termos negativos. Isso causou imprecisão na avaliação de alguns itens de maturidade, o que limitou o diagnóstico mais preciso desse indicador. Outro fator que causou limitação para a eficácia deste instrumento de pesquisa, conforme relatado durante sua aplicação, foi a extensa lista de itens para julgamento dos respondentes, reflexo da quantidade de riscos operacionais identificados (39) e dos itens para avaliação de maturidade de cada processo de TI (120 assertivas ao todo).

Para a avaliação do grau de contribuição dos processos de TI para mitigação de riscos operacionais, adotou-se a escala Likert com número ímpar de elementos, o que em tese gera tendência de resposta para o elemento central da escala. No entanto, conforme os histogramas apresentados (Gráficos 1 a 6), tal tendência não ficou caracterizada, o que ameniza essa limitação do instrumento de pesquisa.

A dificuldade para o alcance da realidade pura é outra limitação deste estudo. A agenda de trabalho dos entrevistados, o sigilo de certas informações e a condução de um único estudo de caso contribuem para a limitação das generalizações analíticas desta seção.

Como sugestão para estudos futuros, com base neste estudo exploratório, podem-se enumerar alguns itens: (i) repetição da pesquisa em outros processos de instituições financeiras, tanto no subsistema de intermediação quanto no subsistema normativo, como é o caso do Banco Central do Brasil; (ii) inclusão de outros processos de tecnologia da informação, como a Gestão de Qualidade e a Gestão de Mudanças, que foram citados durante as entrevistas; (iii) estudo individual dos processos de governança de TI, explorando em detalhes a sua importância para a mitigação dos riscos operacionais; (iv) pesquisa acerca das barreiras para promoção de governança de TI, como a mudança cultural e aspectos de poder; (v) pesquisa empírica para perceber a correlação entre a promoção de governança corporativa

e governança de TI; (vi) pesquisa com pessoas-chave nos processos de TI para perceber a ausência de incentivos para a institucionalização de processos; (vii) pesquisas em organizações de alta confiabilidade, para validar seus pressupostos e buscar a incorporação de outras características desta tipologia.

REFERÊNCIAS BIBLIOGRÁFICAS

A FRAUDE. Direção: James Dearden. Intérpretes: Ewan McGregor, Anna Friel, Yves Beneyton, Betsy Brantley. Inglaterra, 1999. DVD (101 min).

ALBERTIN, Alberto L. e MOURA, Rosa M. **Benefício do Uso da Tecnologia da Informação no Desempenho Empresarial.** Projeto de pesquisa desenvolvido com o apoio do Núcleo de Pesquisa e Publicação da EAESP/FGV. São Paulo: FGV-EAESP, 2004.

ALBERTIN, Alberto L. e ALBERTIN, Rosa M. de M.. Benefício do Uso da Tecnologia da Informação no Desempenho Empresarial**.** In: ALBERTIN, Alberto L. e ALBERTIN, Rosa M. de M. (Orgs). **Tecnologia da Informação – Desafios da Tecnologia da Informação Aplicada aos Negócios**. São Paulo: Atlas, 2005.

ALVES, Carlos A. M. **A divulgação do Risco Operacional segundo recomendações do Comitê da Basiléia: Estudo em bancos com carteira comercial no Brasil.** Dissertação de Mestrado em Administração. Curitiba: UFPR, 2005.

ALVES, Nelson T. H. **Interesses de Investidores e Estruturas de Governança Corporativa de Bancos do Nível 1 da Bovespa.** Dissertação de Mestrado em Administração. Curitiba: UFPR, 2005b.

ARGYRIS, C. Teaching smart people how to learn. **Harvard Business Review**, p. 99-109, May/Jun., 1991.

ASSAF NETO, Alexandre. **Mercado Financeiro.** 6ª. ed. São Paulo: Atlas, 2005.

BABBIE, Earl. **Métodos de Pesquisas de Survey.** Belo Horizonte: Ed. UFMG, 1999.

BACEN. Banco Central do Brasil. **Circular 3.105 – Instituição do Redesconto do Banco Central.** Brasília, 2002. Disponível em <http://www.bcb.gov.br>. Acesso em 20/10/2007.

BACEN. Banco Central do Brasil. **Circular 3.100 – Instituição do STR.** Brasília, 2002b. Disponível em <http://www.bcb.gov.br>. Acesso em 20/10/2007

BACEN. Banco Central do Brasil. **Resolução 3.380 – Estrutura de gerenciamento do risco operacional.** Brasília, junho 2006. Disponível em <http://www.bcb.gov.br>. Acesso em 20/12/2006.

BACEN. Banco Central do Brasil. **Missão Institucional.** 2006b**.** Disponível em <http://www.bcb.gov.br>. Acesso em 15/12/2006.

BACEN. Banco Central do Brasil. **Regimento Interno do BACEN.** 2006c. Disponível em <http://www.bcb.gov.br>. Acesso em 22/12/2006.

BACEN. Banco Central do Brasil. **Catálogo de Mensagens do SPB.** 2007. Disponível em <http://www.bcb.gov.br>. Acesso em 20/10/2007.

BACEN. Banco Central do Brasil. **Sistema de Pagamentos Brasileiro.** 2007b. Disponível em <http://www.bcb.gov.br>. Acesso em 20/10/2007.

BACEN. Banco Central do Brasil. **Glossário.** 2007c. Disponível em <http://www.bcb.gov.br>. Acesso em 01/12/2007.

BACEN. Banco Central do Brasil. **Composição do Sistema Financeiro Nacional.** 2008. Disponível em <http://www.bcb.gov.br/?SFNCOMP >. Acesso em 29/02/2008.

BERGAMINI JR, Sebastião. Controles Internos como um Instrumento de Governança Corporativa. **Revista do BNDES**. Rio de Janeiro: v. 12, n. 24, p. 149-187, Dez. 2005.

BERNSTEIN, Peter L. **Desafio aos Deuses: A Fascinante História do Risco.** 20ª ed. Rio de Janeiro: Elsevier,1997.

BIS. BANK FOR INTERNATIONAL SETTLEMENTS. **Entrega Contra Pagamento em Sistemas de Liquidação de Títulos.** Comitê de Sistemas de Pagamentos e de Liquidação. Setembro de 1992. Disponível em <http://www.bcb.gov.br/htms/spb/DvP-port.pdf>. Acesso em 10/2007.

BIS. BANK FOR INTERNATIONAL SETTLEMENTS. **Framework for the Evaluation of Internal Control Systems.** Basel Committee on Payment Systems. January 1998. Disponível em <http://www.bis.org>. Acesso em 03/2007.

BIS. BANK FOR INTERNATIONAL SETTLEMENTS. **Sound Practices for the Management and Supervision of Operational Risk.** Basel Committee on Banking Supervision. February 2003. Disponível em <http://www.bis.org>. Acesso em 02/2007.

BIS. BANK FOR INTERNATIONAL SETTLEMENTS. **International Convergence of Capital Measurement and Capital Standards – A revised framework.** Basel Committee on Banking Supervision. June 2004. Disponível em <http://www.bis.org>. Acesso em 03/2007.

BIS. BANK FOR INTERNATIONAL SETTLEMENTS. **Enhancing Corporate Governance for Bancking Organizations.** Basel Committee on Banking Supervision. February 2006. Disponível em <http://www.bis.org>. Acesso em 04/2007.

BORITZ, J. Efrim. IS practitioners´ views on core concepts of information integrity**. International Journal of Accounting Information Systems**, n. 6, p. 260-27, 2005.

BOURRIER, Mathilde. An interview with Karlene Roberts**. European Management Journal**, v. 23, n. 1, p. 93-97, February 2005.

BRODBECK, Ângela F.; ROSES, Luis K.; BREI, Vinícius A. **Governança de TI: Medindo o Nível de Serviços Acordados entre as Unidades Usuárias e o Departamento de Sistemas de Informação**. In: XXIX EnAnpad. Brasília, 2004. Anais...

BRODERICK, J. Stuart. ISMS, security standars and security regulations**. Information Security Technical Report**, 2006

BURRELL, Gibson; MORGAN, Gareth. **Sociological Paradigms and Organizational Analysis.** London: Heinemann, 1979.

CAMPANÁRIO, Milton A.; MACCARI, Emerson A.; ALMEIDA, Martinho I. R. **ERP, Corporate Strategy and Knowledge Management**. In: The Business Association of Latin American Studies – BALAS, 2005. Anais...

CARNEIRO, Fábio L.; VIVAN, Gilneu F. A. e KRAUSE, Kathleen. **O novo acordo da Basiléia – um estudo de caso para o contexto brasileiro.** Disponível em <http://www.bcb.gov.br> Acesso em 22/12/2006.

CASTELLS, Manuel. **A Sociedade em Rede.** v. 1, 9. ed. São Paulo: Paz e Terra, 1999

CAZASSA, Eduardo F. Indicadores e Governança Efetiva de TI**.** In: ALBERTIN, Alberto L. e ALBERTIN, Rosa M. de M. (Orgs). **Tecnologia da Informação – Desafios da Tecnologia da Informação Aplicada aos Negócios**. São Paulo: Atlas, 2005.

CIMOLI, Mario e GIUSTA, Marina D. The Nature of Technological Change and its Main Implications on National Systems of Innovation**.** In: Abortes, J. e Dutrénit G. **Innovación, aprendizaje y creación de capacidades tecnologicas**. Universidad Autónoma Metropolitana. Unidade Xochimilco. México, 2003, p. 47-94.

COIMBRA, Fábio C. **Estruturação de Unidade de Gestão de Risco Operacionais em Bancos: um estudo de caso.** Dissertação de Mestrado em Administração. São Paulo: USP, 2006.

COSO, Committee of Sponsoring Organizations of the Treadway Commission. **Internal Control – Integrated Framerowk: Executive Summary.** 1994. Disponível em <http:// www.coso.org> Acesso em 05/2007.

COSO, Committee of Sponsoring Organizations of the Treadway Commission. **Enterprise Risk Management – Integrated Framerowk: Executive Summary.** September, 2004. Disponível em <http://www.coso.org> Acesso em 05/2007.

CRESWELL, John W. **Research Design: qualitative, quantitative and mixed method approaches.** 2. ed. Thousand Oaks: Sage, 2003.

EEDE, Gerd Van D. e WALLE, Bartel Van. Operacional Risk in Incident Management : a Cross-fertilisation Between ISCRAM and IT Governance**. Proceedings of the 2nd. International ISCRAM Conference**. Bélgica, 2005.

EEDE, Gerd Van D.; WALLE, Bartel. Van. e RUTKOWSKI, Anne-Françoise. Dealing with Risk in Incident Management: an Application of High Reliability Theory**. Proceedings of the 39th Hawaii International Conference on System Sciences**, 2006.

FERNANDES, Antônio A. G. **O Sistema Financeiro Nacional Comentado.** São Paulo: Saraiva, 2006.

GARCIA, V. S. G. Gerenciamento de risco em instituições financeiras e o Novo Acordo de Capital**.** In: DUARTE Jr., A.M., VARGA, G. (org.) **Gestão de Riscos no Brasil**. Rio de Janeiro, Financial Consultoria, 2003.

GERKE, Lynne; RIDLEY, Gail. Towards an abbreviated COBIT framework for use in an Australian State Public Sector. **17a. Australian Conference on Information Systems.** Adelaide, 2006.

GIL, Antonio C. **Métodos e Técnicas de Pesquisa Social.** 5. ed. São Paulo: Atlas, 1999.

GIL, Antonio C. **Como Elaborar Projetos de Pesquisa.** 4. ed. São Paulo: Atlas, 2002.

GONÇALVES, José E. L. As Empresas são Grandes Coleções de Processos. **RAE –Revista de Administração de Empresas**, v. 40, n. 1, p. 6-19, Jan/Mar. 2000;

GONÇALVES, Orivaldo. Riscos Operacionais – O grande Desafio para Gestores das Instituições Financeiras. **Disclosure das Transações Financeiras.** Ano IX, n. 131, Maio-Junho, 2007.

GULDENTOPS, Erik. The IT Dimension of Basel II**. Information Systems Control Journal**, v. 6, 2004.

GULDENTOPS, Erik; GREMBERGEN, Win V.; HAES, Steven D. Control and Governance Maturity Survey – Establishing a reference benchmark and a self-assesment tool. **Information Systems Control Journal**, v. 6, 2002.

HARDY, Gary. Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges**. Information Security Technical Report**. 2006.

HATCH, Mary J. **Organization Theory – Modern, Symbolic, and Postmodern Perspectives.** New York: Oxford University Press, 1997.

HOLM, Claus e LAURSEN, Peter B. Risk and Control Developments in Corporate Governance: changing the role of the external auditor? **Corporate Governance**, v. 15, n. 2, March 2007.

ITGI. INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE. **CobiT 4.0 – Control Objectives for Information and related Technology.** 2005. Disponível em <http://www.itgi.org> Acesso em 03/2007.

ITGI. INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE. **IT Control Objectives for Sarbanex-Oxley - the Role of IT in the Design and Implementation of Internal Control Over Financial Reporting.** 2006. Disponível em <http://www.itgi.org> Acesso em 04/2007.

ITGI. INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE. **IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance – Exposure Draft.** 2007. Disponível em <http://www.itgi.org> Acesso em 05/2007.

ITGI. INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE. **CobiT 4.1 – Control Objectives for Information and related Technology.** 2007b. Disponível em <http://www.itgi.org> Acesso em 05/2007.

JIMÉNEZ-JIMÉNEZ, Daniel e CEGARRA-NAVARRO, Juan G. The performance effect of organizational learning and market orientation**. Industrial Marketing Management**, 2006.

KERLINGER, Fred N. **Metodologia da Pesquisa em Ciências Sociais: um tratamento conceitual.** São Paulo: EPU, 1980.

LAINHART IV, John W. Why IT Governance is a Top Management Issue**. The Journal of Corporate Accounting & Finance***,* Jul/Aug 2000.

LASTRES, Helena M. M. e FERRAZ, João C. Economia da Informação, do Conhecimento e do Aprendizado. In: LASTRES, H. M. M. e ALBAGLI, S. (orgs.). **Informação e Globalização na Era do Conhecimento**. Rio de Janeiro: Campus, 1999.

LEMES JR, Antônio B.; CHEROBIM, Ana P.; RIGO, Cláudio M. **Administração Financeira.** São Paulo: Campus, 2005.

MARCONDES, Danilo. **Iniciação à História da Filosofia: dos Pré-socráticos a Wittengestein.** 9ª ed. Rio de Janeiro: Jorge Zahar Ed., 2005.

MARSHALL, Christopher. **Medindo e Gerenciando Riscos Operacionais em Instituições Financeiras.** Rio de Janeiro: Qualitymark, 2002.

MEIRELLES, Anthero M.; ALMEIDA JR, Antônio F.; DATTOLI, José C. B. **Governança Corporativa e Gestão de Riscos no Banco Central do Brasil.** *Mimeo*. 2005.

NELSON, R. e WINTER, S. In Search of Useful Theory of Innovation**. Revista Brasileira da Inovação**, v. 1, n. 2, jul/2002. Rio de Janeiro, 2002.

NEUMAN, Lawrence W. **Social Research Methods: Qualitative and Quantitative Approaches.** 3. ed. Boston: Allyn & Bacon, 1997.

NIST. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Risk Management Guide for Information Technology Systems.** Acesso <csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf> em 09/2007. NIST, 2002.

OCDE. Organização para Cooperação e Desenvolvimento Econômico. **OECD Principles of Corporate Governance.** 2004. Disponível em <http://www.oecd.org> Acesso em 04/2007.

OLIVEIRA, Mirian; OLIVEIRA, Leonardo R.; HANSEN, Peter B.; GASPAROTE, Maurício. **Governança em TI e Competitividade do Arranjo Produtivo Local Coureiro-Calçadista do Rio Grande do Sul**. In: XXIX EnAnpad. Brasília, 2005. Anais...

PEREZ, Carlota. Revoluciones tecnológicas, câmbios de paradigma y de marco socioinstitucional**.** In: Abortes, J. e Dutrénit G. **Innovación, aprendizaje y creación de capacidades tecnológicas**. Universidad Autónoma Metropolitana. Unidade Xochimilco. México, 2003, p. 13-46.

PINOCHET, Luis H. C.; ALBERTIN, Alberto L.; VASCONCELOS, Isabella F. F. G.; MASCARENHAS, André O.; SILVA, Alandey S. L. A **Adoção de Ferramentas de Governança de TI por parte do Conselho de Profissionais de Saúde do Nordeste: uma Análise Crítica com base na Teoria Neo-Institucional**. In: XXIX EnAnpad. Brasília, 2005. Anais...

PINTO, Wellington. **Alta Confiabilidade e Gestão de Risco Operacional em Uma Instituição Financeira: um estudo de caso.** Dissertação de Mestrado – UnB. Brasília, 2005.

PMBOK. Project Management Institute. **Project Management Body of Knowledge.** 2000.

QUEIROZ, Ana C. S e VASCONCELOS, Flavio C. **Organizações, Confiabilidade e Tecnologia**. In: XXIX EnAnpad. Brasília, 2004. Anais...

ROBERTS, Karlene. Managing High Reliability Organizations**. California Management Review**, v. 32, n. 4, p. 101-113. Summer, 1990.

ROBERTS, Karlene e GRABOWSKI, Martha. Organizações, Tecnologia e Estruturação**.** 1996. In: CLEGG, Stewart; HARDY, C.; NORD, W.; CALDAS, M.; FACHIN, R.; FISCHER, T. (Orgs). ***Handbook*** **de Estudos Organizacionais**. v.3. São Paulo: Atlas, 2004.

ROESSING, Rolf von. IT Risk and Business Alignment Under Basel II**. e-Challenges Conference**. Slovenia, October 2005.

SANTOS, Leandro R. Gestão da Maturidade de Processos Essenciais – Convergência para o Futuro. **RAE-Eletrônica**, v. 2, n. 1, jan-jun/2003.

SARBANES, P.; OXLEY, M. **Sarbanes-Oxley Act of 2002**. Disponível em < http: //www .findlaw .com >. Acesso em 04/2007.

SAUNDERS, Mark N.; LEWIS, Philip; THORNHILL, Adrian. **Research Methodos for Business Students.** 2. ed. England: Pearson Education, 2000.

SCHEIN, Edgar H. **Organizational cultures and leadership:** a dynamic view. San Francisco: Jossey-Bass, 1985.

SENGE, P. M. **A quinta disciplina: arte, teoria e prática da organização da aprendizagem**. São Paulo: Nova Cultural, 1990.

SMITH, M. K. **Chris Argyris: theories of action, double-loop learning and organizational learning.** Disponível em <http://www.infed.org/thinkers/argyris.htm>. 2001. Acesso em 05/2007.

SOLMS, Basie von. Information Security Governance: COBIT or ISSO 17799 or both? **Computers & Security**, n. 24, p. 99-104, 2005.

SPINK, Mary J. e LIMA, Helena. Rigor e Visibilidade: A explicitação dos passos da interpretação. In: SPINK, Mary J. (Org.). **Práticas Discursivas e Produção de Sentido no Cotidiano: aproximações teóricas e metodológicas.** São Paulo: Cortez, 2004

SCHUMPETER, Joseph A. **Business Cycles: A Theoretical Historical and Statistical Analysis of the Capitalist Process.** New York: McGraw-Hill, 1939.

TANNENBAUM, Arnold S. **O Controle nas organizações.** Petrópolis: Vozes, 1975.

TORRES, Marcos J. R. **Operacionalidade da Política Monetária no Brasil.** Tese de Doutorado em Economia. Campinas: UNICAMP, 1999.

TURNBULL, S. Corporate governance: Its scope, concerns and theories. **Scholarly Research and Theory Papers**, vol. 5, No. 4, p. 180-205, October, 1997

VERGARA, Sylvia C. **Métodos de Pesquisa em Administração.** São Paulo: Atlas, 2005.

VERGARA, Sylvia C. **Projetos e Relatórios de Pesquisa em Administração.** 7 ª ed. São Paulo: Atlas, 2006.

WEICK, Karl e WESTLEY, Frances. Aprendizagem Organizacional: confirmando um oxímoro**.** 1996. In: CLEGG, Stewart; HARDY, C.; NORD, W.; CALDAS, M.; FACHIN, R.; FISCHER, T. (Orgs). ***Handbook*** **de Estudos Organizacionais**. v.3. São Paulo: Atlas, 2004.

WEICK, Karl e SUTCLIFFE, K. **Managing the Unexpected: Assuring high performance in the age of complexity.** San Francisco: Jossey-Bass, 2001.

WEILL, Peter e ROSS, Jeanne W. **Governança de TI**. São Paulo: M Books, 2006.

YIN, Robert K. **Estudo de Caso: planejamento e métodos.** 3. ed. Porto Alegre: Bookman, 2005.

ZORELLO, Gilberto. **Metodologias COBIT e ITIL e as perspectivas do Modelo de Alinhamento Estratégico de TI**. In: XII SIMPEP. Bauru, 2005. Anais...

ANEXO A – NÍVEIS DE MATURIDADE DE PROCESSOS

Os processos selecionados para a pesquisa empírica possuem os seguintes níveis e respectivos atributos de maturidade:

NÍVEIS DE MATURIDADE DE PROCESSO **(0)** Não existe **(1)** Inicial **(2)** Repetido **(3)** Definido **(4)** Gerenciado **(5)** Otimizado	
Domínio: PLANEJAMENTO E ORGANIZAÇÃO	
Processo: Avaliação e Gestão de Riscos de TI	
0	O processo de avaliação e gestão de riscos de TI (GR) não é identificado como relevante.
1	Os riscos são gerenciados de maneira *ad hoc*. As avaliações de riscos de projeto são de forma individual, projeto a projeto. Os riscos identificados raramente são designados para gerentes específicos. Os riscos cotidianos de TI raramente são discutidos em reuniões. Quando o risco é considerado, sua mitigação é inconsistente. A consciência de risco é emergente.
2	Uma abordagem de GR está em desenvolvimento e é implementada de acordo com cada gerente. A GR é usualmente de alto nível e para projetos mais importantes ou em resposta a problemas. Processos de mitigação de risco estão sendo implantados quando há a identificação de risco.
3	Há uma política organizacional definindo quando e como conduzir a GR. O processo é documentado. Ocorrem treinamentos de GR. As decisões sobre seguir os procedimentos e receber treinamento são individuais. A metodologia para GR é convincente e assegura que riscos-chave para o negócio são identificados. Processos de mitigação de risco são usualmente instituídos uma vez que os riscos são identificados. A descrição de cargos considera as responsabilidades de GR.
4	Há procedimentos padrões para GR. Exceções são reportadas à gerência de TI. A responsabilidade pela GR é de nível sênior. Riscos são avaliados e mitigados no plano individual de projetos e também alinhados à operação geral de TI. Mudanças no ambiente de negócios e de TI que possam afetar os cenários de riscos de TI são alertados para a gerência. A gerência é habilitada para monitorar a posição de risco e tomar decisões em função da exposição desejada. Todos os riscos identificados possuem um funcionário responsável e as gerências sênior e de TI determinam o nível de risco tolerado. A gerência de TI desenvolve medidas padrão para a GR definição de *trade-off* risco/retorno. O orçamento para projeto de gestão de risco operacional é reavaliado periodicamente. Há um banco de dados para gestão de riscos e parte do processo é automatizada. A gerência de TI considera estratégias de mitigação de risco.
5	O processo de GR é estruturado, reforçado em toda a organização e bem gerenciado. Boas práticas são aplicadas em toda a organização. A captura, análise e informação de dados para GR é altamente automatizada. Há orientação de líderes nesse campo e a organização realiza trocas de experiências. A GR é integrada em todas as linhas de negócio. Os gerentes detectam e atuam quando decisões de investimento em TI são feitas sem considerar o plano de gerenciamento de riscos. A gerência continuamente avalia estratégias de mitigação de

	riscos.
Processo: Gestão de Projetos	
0	Técnicas de gestão de projetos (GP) não são utilizadas.
1	O uso de técnicas e metodologias de GP de TI é individual. Decisões críticas de GP são feitas sem a consulta ao usuário do projeto. Os usuários pouco se envolvem na definição de projetos de TI. Não há estrutura clara para a GP de TI. Papéis e responsabilidades para a GP não são definidos. Projetos, cronogramas e metas são deficientemente definidos. Não há comparação entre despesas de projetos e orçamentos.
2	A gerência sênior busca conscientizar a necessidade de GP de TI. Algumas técnicas e métodos são utilizados, caso a caso. Os projetos de TI definem informalmente objetivos de negócio e técnicas. Há envolvimento limitado de *stakeholders* na GP de TI. Algumas orientações iniciais são desenvolvidas para aspectos de GP. A aplicação das orientações é a cargo de cada gerente de projeto.
3	O processo e a metodologia de GP de TI são estabelecidos e comunicados. Os projetos de TI são definidos com objetivos de negócio e técnicos. Gerentes seniores de TI e de negócio estão iniciando comprometimento na GP de TI. Existe um escritório de gestão de projetos de TI, com papéis e responsabilidades iniciais definidos. Os projetos de TI são monitorados e com medidas atualizadas de cronograma, orçamento e desempenho. Treinamento para GP é realizado, mas resultado de iniciativas individuais. Há início de GP por portfólio.
4	Métricas de projeto e lições aprendidas são consideradas. A GP é medida e avaliada em toda a organização, não somente na área de TI. Melhorias são realizadas no processo de GP, formalizadas, comunicadas e treinadas nas equipes. São estabelecidos critérios para a avaliação de sucesso em cada meta de projeto. Valor e risco são medidos antes e após a conclusão do projeto. Os projetos cada vez mais observam objetivos do negócio e não só de TI. Há apoio ativo de gerentes seniores e *stakeholders* à disciplina de gestão de projetos. O escritório de projetos possui planejamento relevante para treinamento da assessoria e área de TI.
5	Uma metodologia provada, de ciclo completo de vida é implementada, reforçada e integrada na cultura organizacional. São implementadas iniciativas de identificar e institucionalizar melhores práticas de GP. São definidas e implementadas estratégias para documentação de desenvolvimentos e operação de projetos. Há um escritório integrado de gestão de projetos responsável por projetos e programas, do início e até após a implementação. Planejamento de programas e projetos asseguram a melhor utilização de recursos de TI.
Processo: Gestão de Recursos Humanos de TI	
0	Não há consciência sobre alinhamento de gestão de recursos humanos de TI (GRH) ao planejamento organizacional.
1	A gerência reconhece a necessidade de GRH. O processo de GRH é informal e reativo. O processo de GRH é operacionalmente focado, na contratação e gerência de pessoal. A consciência está em desenvolvimento, considerando o impacto que as rápidas mudanças tecnológicas e a crescente complexidade de soluções têm nas habilidades necessárias para TI.
2	Há uma abordagem de nível tático para a contratação e gestão de pessoas, dirigida por necessidades específicas de projetos. Treinamentos informais são realizados para novos

	contratados.
3	A GRH é definida e documentada. Existe um plano para GRH. Há uma abordagem estratégica para a contratação e gestão de pessoas. Existe um plano formal de treinamento para a capacitação necessária. É estabelecido um programa de rotatividade para expandir as habilidades técnicas e de negócio.
4	A responsabilidade pelo plano de GRH é designada para um grupo específico, com experiência necessária para desenvolver e manter o plano. O processo de desenvolvimento do plano de GRH é responsivo a mudanças. Medidas padronizadas existem para identificar desvios relacionados ao plano de GRH, com ênfase no crescimento e *turnover* do grupo de profissionais de TI. Revisões de desempenho e compensação de RH estão sendo desenvolvidas e comparadas com outras organizações e boas práticas. A GRH é proativa, considerando o desenvolvimento na carreira.
5	O plano de GRH é continuamente atualizado para atender às mudanças de requisitos de negócio. A GRH é integrada com o plano de tecnologia, assegurando ótimo uso de habilidades disponíveis de TI. A GRH é integrada e responsiva às diretrizes estratégicas da organização. Componentes da GRH são consistentes com as boas práticas, como compensação, avaliação de desempenho, transferência de conhecimento, treinamento. Programas de treinamento são desenvolvidos para todas os novos padrões tecnológicos e produtos, para a sua implantação na organização.
Domínio: ENTREGA E SUPORTE	
Processo: Continuidade de Serviço	
0	A continuidade de serviço (CS) não é considerada relevante.
1	As responsabilidades pela CS são informais. A conscientização está iniciando. O foco da gestão é nos recursos de infra-estrutura e não nos serviços de TI. Usuários implementam soluções temporárias em resposta a falta de serviços de TI. As respostas são reativas e não preparadas. Planos de interrupção são agendados, mas levam em consideração necessidades de TI somente, e não de negócio.
2	São designadas responsabilidades pela CS. As abordagens para garantir CS são fragmentadas. Informações sobre disponibilidade de sistemas é esporádica, pode ser incompleta e não consideram impactos no negócio. Não há plano CS de TI documentado, embora os principais serviços sejam conhecidos. Existe um inventário dos sistemas e componentes críticos, mas pode não ser confiável. Práticas de CS estão emergindo, mas o sucesso depende de indivíduos.
3	Há prestação de contas sobre CS. Responsabilidades pelo planejamento e testes de CS são claramente identificadas. O plano de continuidade de TI é documentado e baseado nos aspectos críticos do sistema e nos impactos no negócio. Há informações periódicas sobre testes de CS. Há iniciativas individuais para seguir padrões e receber treinamentos para incidentes e desastres. A gerência comunica consistentemente a necessidade para planejamento de CS. Componentes de alta disponibilidade e redundância de sistemas estão sendo aplicados. Um inventário de componentes e sistemas críticos é manutenido.
4	São reforçadas as responsabilidades por CS. A responsabilidade por manter o plano de CS é designada. Atividades de manutenção são baseadas nos resultados de testes de CS, boas práticas internas e mudanças de ambientes de TI e de negócio. Dados estruturados sobre CS são coletados, analisados e informados. Treinamento formal e obrigatório é providenciado para processos de CS. Práticas de disponibilidade e plano de CS se complementam.

	Incidentes de descontinuidade são classificados e reconhecidos. Objetivos e métricas para CS têm sido desenvolvidos, mas ainda medidos de forma inconsistente.
5	Os processos integrados de CS consideram *benchmarking* e melhores práticas externas. O plano de continuidade de TI é integrado com o plano de continuidade de negócio e manutenido rotineiramente. O requisito por CS é assegurado pelos principais fornecedores. Ocorrem testes globais de planos de CS de TI e os resultados retroalimentam o plano. Coleta e análise de dados são continuamente usadas para a melhoria do processo. Práticas de disponibilidade e plano de CS são totalmente alinhadas. A gerência assegura que um desastre ou incidente maior não ocorrerá em função de uma falha pontual. Objetivos e métricas de CS são usadas de forma sistemática. A gerência ajusta o plano de CS em resposta às medidas.
Processo: Segurança de Sistemas de TI	
0	A organização não reconhece o processo de segurança de sistemas de TI (SS).
1	A consciência da necessidade de segurança é individual. A segurança de TI é tratada de forma reativa e não é mensurada. As responsabilidades por SS não são claras. Respostas para rupturas de SS são imprevisíveis.
2	Responsabilidades são designadas para um coordenador de SS, embora sua autoridade seja limitada. A consciência da necessidade de segurança é fragmentada e limitada. Informações relevantes sobre SS são produzidas, mas não analisadas. Serviços terceirizados podem não atender às necessidades específicas de segurança da organização. Políticas de segurança têm sido desenvolvidas, mas as competências e ferramentas são inadequadas. O relatório de SS é incompleto. Iniciativas individuais de treinamento são encontradas. A área de negócio não vê a SS como importante para seu domínio.
3	A conscientização sobre SS é promovida pela gerência. Políticas e procedimentos de SS são definidos e alinhados. Responsabilidades são designadas, mas não consistentemente reforçadas. Existe um plano de SS orientado por análise de risco. Informações sobre segurança não contêm foco claro no negócio. Testes de segurança *ad hoc* são executados. Treinamentos de segurança para TI e para o negócio existem, mas agendados e gerenciados informalmente.
4	Responsabilidades por SS são claramente designadas, gerenciadas e reforçadas. Análises de risco e de impacto são consistentemente realizadas. É obrigatória a exposição a métodos para promoção de SS. Identificação, autenticação e autorização de usuários são padronizadas. Certificação em segurança é recomendada para assessores responsáveis pela auditoria e gestão de SS. Testes de segurança utilizam processos padronizados e formalizados. Processos de SS são coordenados conjuntamente com outras funções de segurança na organização. Informações sobre SS são ligadas a objetivos de negócio. Treinamentos de SS são conduzidos nos ambientes de TI e de negócio. Treinamento de SS é planejado e gerenciado de forma que responda a necessidades do negócio e perfis de risco definidos. Métricas e objetivos foram definidos mas ainda não são utilizados.
5	SS é uma responsabilidade conjunta das gerências de TI e de negócio, e integrada com os objetivos corporativos de segurança de negócio. Os requisitos de SS são claramente definidos, otimizados e incluídos no plano de segurança. Usuários são comprometidos com a definição de requisitos de SS, e funções de segurança são integradas com aplicações na fase de projeto. Incidentes de segurança são prontamente detectados por procedimentos suportados em ferramentas de automação. Avaliações periódicas de SS são conduzidas para avaliar a eficácia do plano de segurança. Informações sobre ameaças são sistematicamente coletadas e analisadas. Controles adequados para mitigar riscos são prontamente

	comunicados e implementados. Testes de segurança, análise de causas de incidentes e identificação pró-ativa de riscos são usados para melhoria de processos. Dados para gestão da SS são coletados, medidos e comunicados. A gerência usa as medidas para ajustar o plano de segurança.
Processo: Gestão de Dados	
0	Dados não são reconhecidos como ativos ou recursos da organização. Não há designação de responsabilidade pela gestão de dados (GD).
1	A organização reconhece a necessidade de efetiva GD. Há uma abordagem *ad hoc* para especificação de requisitos para GD, mas procedimentos formais não ocorrem. Não há treinamentos específicos sobre GD. Responsabilidade pela GD não é clara. Há procedimentos de backup e restauração de dados.
2	Existe a conscientização sobre a importância da GD em toda a organização. A identificação de proprietários de dados está iniciando. Requisitos de segurança para GD são documentados por iniciativas individuais. Há algum monitoramento sobre desempenho de atividades de GD. As responsabilidades são informais e designadas para indivíduos-chave.
3	A necessidade de GD é entendida e aceita na área de TI e em toda a organização. Responsabilidades pela GD são definidas. Propriedade de dados é designada para as partes responsáveis, que controlam sua integridade e segurança. Procedimentos de GD são formalizados e algumas ferramentas são adotadas. Medidas básicas de desempenho são definidas. Treinamentos para GD são realizados com freqüência.
4	As responsabilidades pela GD são claramente definidas, designadas e comunicadas na organização. Procedimentos são formalizados e amplamente conhecidos, e o conhecimento é compartilhado. O uso de ferramentas para GD é emergente. Objetivos e indicadores de desempenho são acertados com os usuários e monitorados por meio de um processo bem definido. Treinamento formal para toda a equipe de GD é realizado.
5	Os requisitos para eficiência e eficácia de GD são explorados de maneira proativa. As responsabilidades pela GD e propriedade de dados são claramente estabelecidas, difundidas e atualizadas periodicamente. Procedimentos de GD são formalizados e amplamente conhecidos. Ferramentas sofisticadas são usadas com alto grau de automatização de GD. Objetivos e indicadores de desempenho de GD são relacionados aos objetivos de negócio e consistentemente monitorados. Oportunidades para melhoria na GD são constantemente exploradas. O treinamento para a área de GD está institucionalizado.
Domínio: MONITORAMENTO E AVALIAÇÃO	
Processo: Avaliação e Monitoramento de Controles Internos	
0	A organização não possui procedimentos para monitorar a eficácia de controles internos de TI (CI).
1	A gerência reconhece a necessidade para gerência e controle de TI. A experiência individual para avaliação de CI é aplicada de maneira *ad hoc*. A gerência de TI não designou formalmente a responsabilidade para monitorar a eficácia de CI. Avaliações de CI são conduzidas como parte tradicional de auditorias financeiras, com metodologias e competências que não refletem a necessidade da função de serviços de informação.
2	A organização usa controle informal para iniciar ações de correção. Avaliação de CI é dependente de habilidades individuais. A consciência sobre CI tem aumentado. A gestão de

	serviços de informação realiza monitoramento sobre a eficácia do que ela acredita ser CI críticos. Metodologias e ferramentas para monitorar CI estão no início de utilização, mas não como parte de um plano. Riscos específicos para o ambiente de TI são identificados com base nas habilidades individuais.
3	A gerência suporta o monitoramento de CI. Políticas e procedimentos são desenvolvidos para avaliar e informar sobre atividades de CI. Há um programa definido de educação e treinamento para monitoramento de CI. O processo é definido para auto-avaliação e para revisões de garantia de CI. Ferramentas são utilizadas mas não necessariamente integradas em todos os processos. Políticas de avaliação de riscos de processos de TI estão sendo usadas na estrutura de controle desenvolvida especificamente para a organização de TI. Riscos específicos de processo e políticas de mitigação são definidos.
4	A gerência implementa uma estrutura para monitoramento de CI. A organização estabelece níveis de tolerância para o processo de monitoramento. São implementadas ferramentas para padronizar avaliações e detectar exceções automaticamente. A função de CI é formalmente estabelecida, com profissionais certificados utilizando uma estrutura de controle formal aprovada pela gerência sênior. Assessores de TI capacitados participam das avaliações de CI. Uma base histórica de conhecimentos de CI é estabelecida. Revisões pontuais para monitoramento de CI são estabelecidas.
5	A gerência estabelece um programa organizacional para melhoria contínua que considera lições aprendidas e boas práticas para monitoramento de CI. A organização usa ferramentas atualizadas e integradas, que permite avaliação eficaz de CI e rápida detecção de incidentes de monitoramento de CI. Compartilhamento de conhecimento específico para a função de serviços de informação é formalmente implementado. *Benchmarking* com padrões da indústria e boas práticas é formalizado.
Processo: Promoção de Governança de TI	
0	Não há consciência sobre a importância da governança de TI (GTI).
1	Existem abordagens *ad hoc* aplicadas individualmente. A abordagem gerencial é reativa e existe comunicação esporádica e inconsistente sobre questões e metodologias para GTI. A gerência tem somente uma indicação aproximada sobre como a TI contribui para o desempenho do negócio. A gerência responde reativamente a incidentes que causaram perda ou embaraço para a organização.
2	Há consciência sobre questões de GTI. Estão em desenvolvimento atividades de GTI e indicadores de desempenho, que incluem planejamento de TI e processos de entrega e monitoramento. Processos selecionados são identificados para melhoria baseada em decisões individuais. A gerência identifica medidas básicas, técnicas e métodos de avaliação de GTI, entretanto o processo não ocorre em toda a organização. Comunicação e responsabilidade sobre padrões de GTI são individuais. A GTI é limitada devido à falta de especialização em suas funcionalidades.
3	A conscientização é compreendida e a gerência comunica a toda a organização. Uma linha de base com indicadores de GTI é desenvolvida e documentada, na qual são definidas relações entre medidas de resultado e indicadores de desempenho. Procedimentos são padronizados e documentados. A gerência comunica os padrões e há treinamento. Ferramentas são identificadas para auxiliar a GTI. Painéis são definidos como parte de *balanced score cards* de TI. Entretanto, o treinamento e uso é deixado a cargo individual. Processos podem ser monitorados, mas desvios são improváveis de serem detectados pela gerência.

4	Há um profundo entendimento sobre questões de GTI. Há uma clara compreensão de quem é o cliente e responsabilidades são definidas e monitoradas. Responsabilidades e proprietários de processos são claramente identificados. Processos de TI e GTI são alinhados à estratégia de TI e de negócio. Melhorias em processos de TI são baseadas em compreensão quantitativa, e é possível monitorar e medir conformidade a procedimentos e métrica de processos. Todos os *stakeholders* são conscientes do risco, da importância de TI e das oportunidades que ela pode oferecer. A gerência define níveis de tolerância para operação dos processos. Há uso tático limitado da tecnologia, com base em técnicas maduras e ferramentas padrão. GTI foi integrada ao plano estratégico e operacional, e aos processos de monitoramento. Indicadores de desempenho de GTI são registrados e acompanhados, levando a melhorias na organização. Prestação de contas de processos-chave é concebida, e a gestão é suportada por medidas-chave de desempenho.
5	Há um avançado entendimento de questões e soluções de GTI. Treinamento e comunicação são suportados por técnicas e conceitos maduros. Processos são refinados a níveis de boas práticas da indústria, baseados em resultados de melhorias contínuas e modelagem de maturidade em outras organizações. A implementação de políticas leva a uma rápida adaptação de pessoas e processos organizacionais a requisitos de GTI. Em todos os problemas e desvios são analisadas as causas básicas, e ações eficientes são identificadas e iniciadas. A TI é usada de maneira extensiva, integrada e otimizada para automatizar o fluxo de trabalho, em direção à melhoria de qualidade e eficácia. Os riscos e retornos de processos de TI são identificados, balanceados e comunicados na organização. Monitoramento, auto-avaliação e comunicação sobre expectativas de GTI são pervasivas em toda a organização. Governança corporativa e GTI são estrategicamente ligadas, alavancando tecnologia, recursos humanos e financeiros para aumentar a vantagem competitiva da organização. Atividades de GTI são integradas ao processo de governança corporativa.

Fonte: Adaptado de ITGI (2007a)

ANEXO B – PROTOCOLO DE ENTREVISTA: Descrição do Processo de Negócio

A. Introdução ao estudo de caso

Área de concentração: Risco Operacional, Governança de Tecnologia da Informação, Organizações de Alta Confiabilidade

B. Apresentação dos objetivos da pesquisa

Objetivos do estudo: descrever o processo de negócio; identificar riscos operacionais; investigar a contribuição de processos de controle de Governança de TI para a mitigação de riscos operacionais; avaliar a maturidade dos processos de controle; identificar características de alta confiabilidade na gestão do risco operacional.

Objetivos desta etapa: descrever o processo de negócio.

C. Procedimentos da coleta de dados

Local 1: Departamento de Operações Bancárias e Sistema de Pagamentos – DEBAN
Edifício Sede – Setor de Autarquias Sul – Brasília-DF
Local 2: Departamento de Operações do Mercado Aberto – DEMAB
Av. Pres. Vargas, 730 – Centro – Rio de Janeiro-RJ

Apresentar o estudo de caso e salientar o sigilo no tratamento e divulgação dos dados. Solicitar o consentimento para gravação das entrevistas.

D. Questões desta etapa

D1. Descrever, em linhas gerais, o processo de Redesconto Bancário (Redesconto)
D2. Perceber as mudanças na operacionalização do Redesconto após a implantação do SPB
D3. Listar os sistemas de informação utilizados no processo de Redesconto
D4. Perceber as vantagens e desvantagens com a nova forma de operacionalização
D5. Aprofundar o funcionamento do Redesconto no SPB
D6. Perceber a importância do canal SPB-Selic
D7. Levantar os riscos do processo de negócio em foco
D8. Entender as diferenças dos modelos de liquidação
D9. Levantar os riscos financeiros presentes no processo de liquidação

ANEXO C – PROTOCOLO DE ENTREVISTA: Riscos Operacionais

A. Introdução ao estudo de caso

Área de concentração: Risco Operacional, Governança de Tecnologia da Informação, Organizações de Alta Confiabilidade

B. Apresentação dos objetivos da pesquisa

Objetivos do estudo: descrever o processo de negócio; identificar riscos operacionais; investigar a contribuição de processos de controle de Governança de TI para a mitigação de riscos operacionais; avaliar a maturidade dos processos de controle; identificar características de alta confiabilidade na gestão do risco operacional.

Objetivos desta etapa: identificar riscos operacionais relacionados à TI

C. Procedimentos da coleta de dados

Local 1: Departamento de Operações Bancárias e Sistema de Pagamentos – DEBAN
Edifício Sede – Setor de Autarquias Sul – Brasília-DF
Local 2: Departamento de Operações do Mercado Aberto – DEMAB
Av. Pres. Vargas, 730 – Centro – Rio de Janeiro-RJ

Apresentar o estudo de caso e salientar o sigilo no tratamento e divulgação dos dados. Solicitar o consentimento para gravação das entrevistas.

D. Questões desta etapa

Negócio: ameaças, impactos
Tecnologia: vulnerabilidades, probabilidades

D1. Caracterizar todos os sistemas de informação (SI) utilizados para apoio ao processo de Redesconto (missão, interfaces, software, hardware, dados, pessoas)
D2. Levantar as falhas operacionais já apresentadas pelos SI: causas, consequências, desdobramentos, ações corretivas
D3. Identificar as fontes de ameaças potenciais ao SI (históricos interno e externo; ameaças acidentais ou intencionais; ameaças naturais, ambientais ou humanas)
D4. Identificar as fontes de vulnerabilidades do SI (avaliações anteriores, auditorias, testes de segurança, requisitos de segurança)

> - Vulnerabilidade: "uma fraqueza no projeto, implementação ou procedimentos de segurança de sistemas, ou em controles internos, que pode ser explorada (acidentalmente disparada ou explorada intencionalmente) e resulta em uma quebra de segurança ou violação da política de segurança de sistemas"

D5. Identificar os controles implementados ou planejados: técnicos (incorporados em hardware ou software) ou não técnicos (políticas, procedimentos), nas categorias de prevenção ou de detecção.

ANEXO D – PROTOCOLO DE ENTREVISTA: Processos de Controle

A. Introdução ao estudo de caso

Área de concentração: Governança de Tecnologia da Informação (riscos, controle)

B. Apresentação dos objetivos da entrevista

Objetivos desta etapa: investigar a importância dos processos de controle de GTI ; avaliar a aplicabilidade dos modelos de maturidade para a gestão de processos;

C. Procedimentos da coleta de dados

Local 1: Departamento de Auditoria Interna – DEAUD
Edifício Sede – Setor de Autarquias Sul – Brasília-DF

Apresentar o estudo de caso e salientar o sigilo no tratamento e divulgação dos dados. Solicitar o consentimento para gravação das entrevistas.

D. Questões desta etapa

D1. Investigar as funções da auditoria interna com relação à Governança de TI (GTI), na abordagem atual de avaliação de controles internos sob a ótica de risco.

Propagação de conceitos; Avaliação de Controle Interno: ambiente de controle, avaliação de risco, atividades de controle, informação e comunicação, monitoramento.

D2. Verificar a adoção de modelos de GTI na organização e a sua aceitação

D3. Verificar se e por que os processos do domínio de Monitoramento e Avaliação do modelo Cobit são reconhecidos pela Auditoria como importantes e relacionados a aspectos de controle interno

D4. Os processos de governança de TI (Gestão de Projetos, Continuidade de Serviços, Gestão de Dados, Gestão de Riscos, Segurança de Sistemas, Gestão de RH de TI) mostraram-se importantes para a mitigação de riscos operacionais no processo de redesconto bancário. Diante disso, qual a importância dos processos de controle: ME 2- Monitoramento e Avaliação de Controles Internos e ME 4 – Promoção de GTI ?

D5. Investigar como os processos de Monitoramento/Controle são conduzidos na organização (área de TI, auditoria, ambas)

D6. Analisar o uso dos modelos de maturidade de GTI na organização

D7. Analisar a adequação da distribuição de atributos de gestão nos níveis de maturidade: consciência e comunicação; políticas, planos e procedimentos; ferramentas e automação; habilidades e competência; responsabilidade e prestação de contas; e estabelecimento de objetivos e medidas de desempenho.

D8. Investigar a aplicabilidade do modelo de maturidade Cobit para a gestão de processos (pré-requisitos, barreiras, dificuldades de aplicação, custos e benefícios, coerência dos resultados, adaptação cultural, flexibilidade e customização, ferramentas de apoio, uso na indústria)

ANEXO E – PROTOCOLO DE ENTREVISTA: Alta Confiabilidade

A. Introdução ao estudo de caso

Área de concentração: Risco Operacional, Governança de Tecnologia da Informação, Organizações de Alta Confiabilidade

B. Apresentação dos objetivos da pesquisa

Objetivos do estudo: descrever o processo de negócio; identificar riscos operacionais; investigar a contribuição de processos de controle de Governança de TI para a mitigação de riscos operacionais; avaliar a maturidade dos processos de controle; identificar características de alta confiabilidade na gestão do risco operacional.

Objetivos desta etapa: descrever o processo de negócio.

C. Procedimentos da coleta de dados

Local 1: Departamento de Operações Bancárias e Sistema de Pagamentos – DEBAN
Edifício Sede – Setor de Autarquias Sul – Brasília-DF
Local 2: Departamento de Operações do Mercado Aberto – DEMAB
Av. Pres. Vargas, 730 – Centro – Rio de Janeiro-RJ

Apresentar o estudo de caso e salientar o sigilo no tratamento e divulgação dos dados. Solicitar o consentimento para gravação das entrevistas.

D. Questões desta etapa

D1. Investigar a presença de processos de monitoramento, detecção e prevenção de falhas operacionais
D2. Analisar a presença de sequências não planejadas ou inesperadas, não visíveis ou compreensíveis imediatamente
D3. Conhecer o grau de interdependência entre os sistemas para o redesconto, bem como entre as unidades envolvidas no processo de negócio
D4. Investigar características organizacionais

D4.1 Comunicação
D4.1.1 Analisar a qualidade e diversidade no processo de comunicação para o entendimento de papéis, responsabilidades, discussão sobre melhorias no sistema
D4.1.2 Perceber a existência de espaços de não-punição para a análise de falhas ou quase falhas e diminuição de incertezas
D4.1.3 Entender se os participantes sabem com quem se comunicar em caso de dúvidas no redesconto

D5.1 Tomada de Decisão e Estrutura Organizacional
D5.1.1 Entender se há predomínio de controles burocráticos ou estilos colegiado
D5.1.2 Compreender o que prevalece em situação de emergência: experiência ou posto

D6.1 Cultura

D6.1.1 Analisar qual o procedimento na chegada de novos funcionários
D6.1.2 Analisar a existência de rotinas em contra-posição a novas situações
D6.1.3 Perceber se há consenso de que sempre há algo a apreender
D6.1.4 Perceber o ponto de vista acerca do reconhecimento de possíveis falhas de sistema
D6.1.5 Entender como grandes e pequenos erros são tratados
D6.1.6 Verificar se existem normas que balizam os procedimentos
D6.1.7 Verificar se há comprometimento em todos os níveis com a questão de falhas

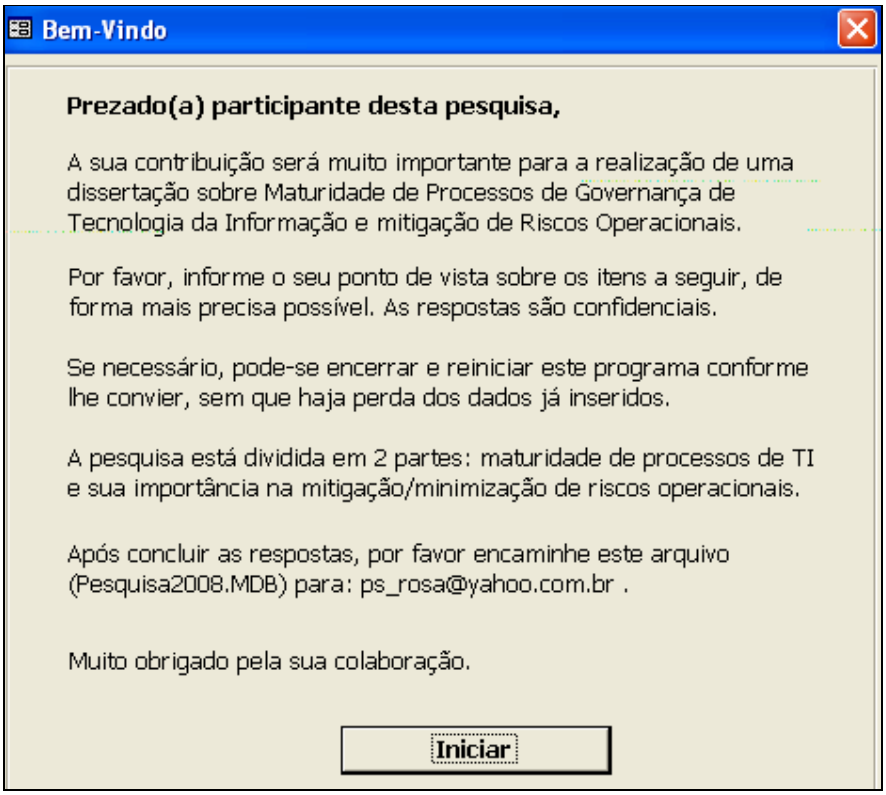
D7.1 Aprendizagem
D7.1.1 Entender a aprendizagem individual e a ocorrência de aprendizagem organizacional
D7.1.2 Verificar a intensidade de mudança ambiental
D7.1.3 Perceber a consciência sobre as reavaliações de pressupostos, tarefas e decisões para a melhoria contínua de monitoramento
D7.1.4 Verificar qual a importância dos atributos confiabilidade e flexibilidade
D7.1.5 Entender o ponto de vista sobre o oxímoro organizar e apreender

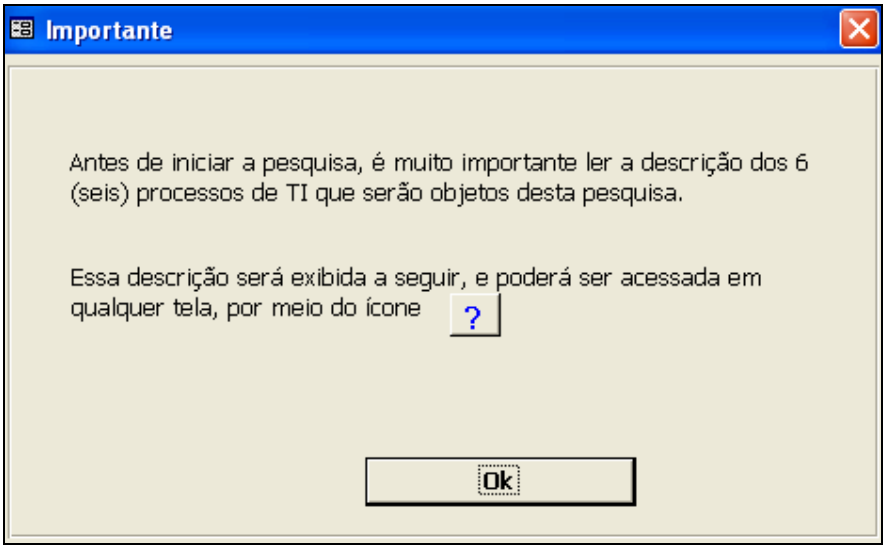
D8.1 Verificar se alguma outra característica pode ser colocada como importante para OAC

D9. Analisar se ocupação com falhas ou possibilidade de falhas é reativa ou pró-ativa
D10. Entender se as rotinas são simplificadas ao máximo ou busca-se a segregação de complexidades, com manutenção de controles
D11. Verificar a implantação de contingências para a manutenção das operações
D12. Verificar se especialistas são incentivados à participação nas decisões, independentemente de seu posto

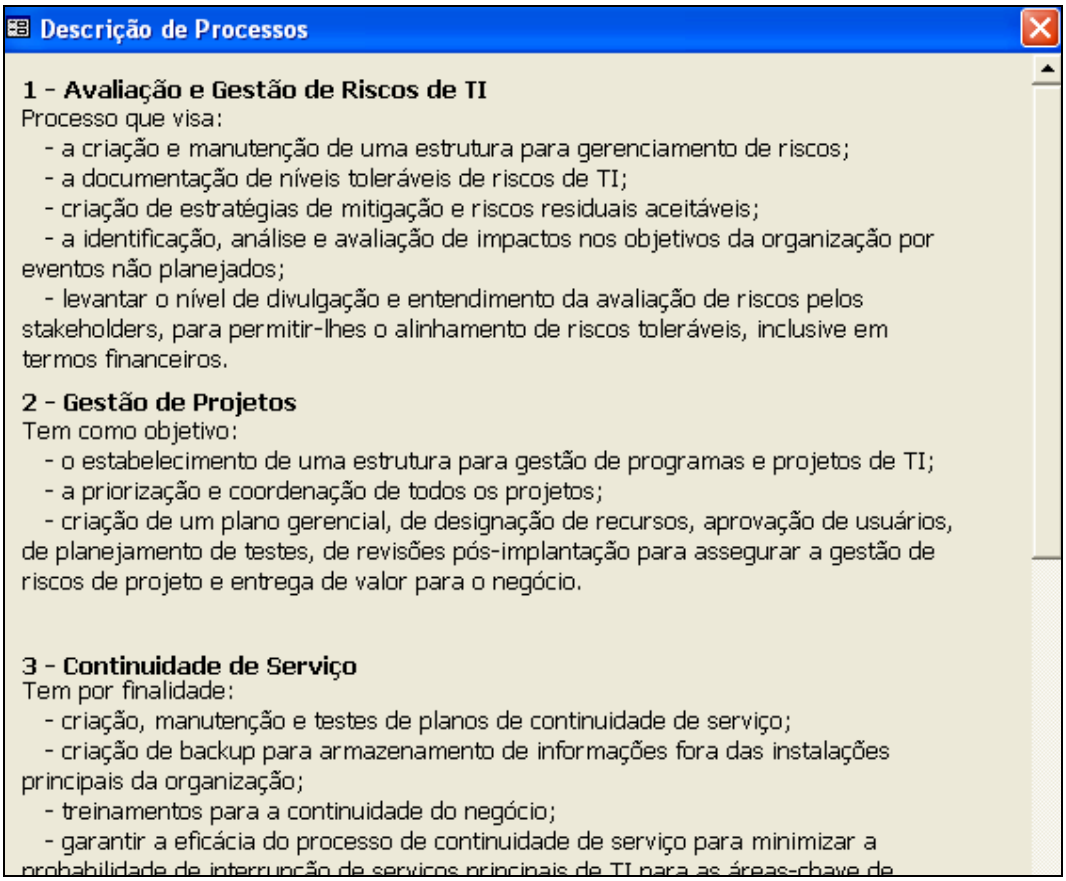
ANEXO F – QUESTIONÁRIO ELETRÔNICO: Processos de TI e Maturidades

- ✓ Informações Iniciais

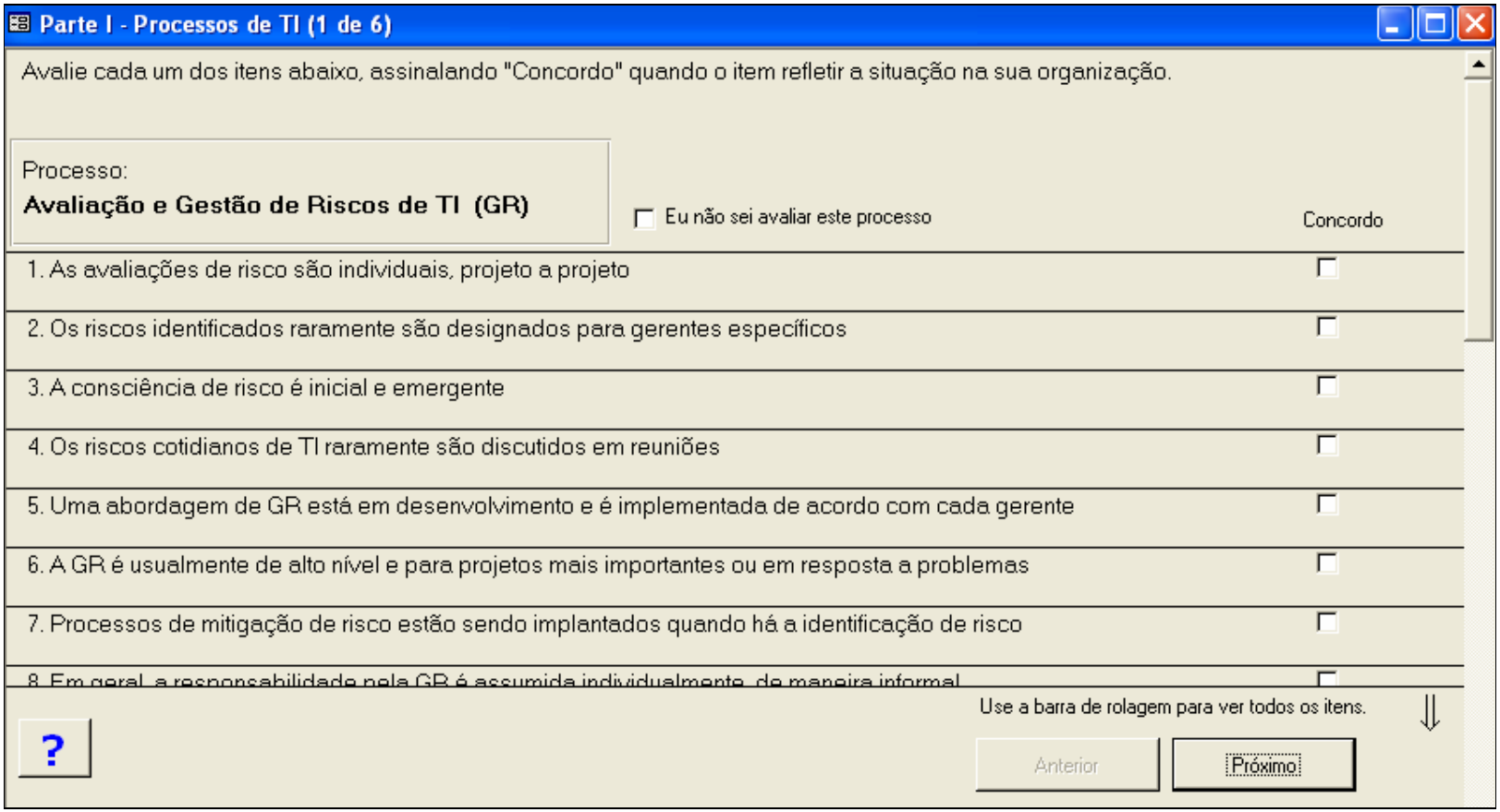




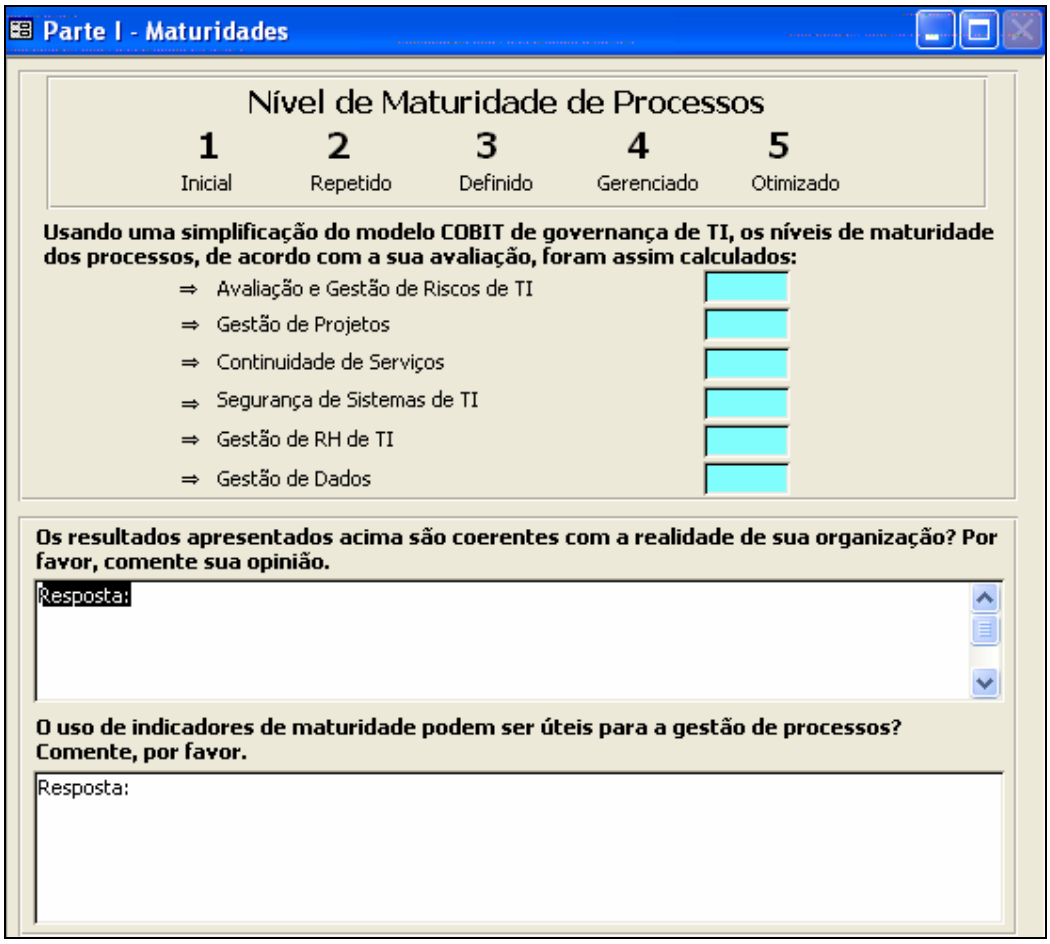
- ✓ Descrição dos processos a serem avaliados



✓ Simulação do modelo de maturidade de cada um dos seis processos de TI.



✓ Apresentação dos resultados e análise da aplicabilidade do modelo de maturidade



- ✓ Avaliação de cada um dos seis processos de TI com relação à importância para mitigação de cada um dos riscos operacionais do processo de negócio